HACKER JOURNAL

Anno 2 – N. 25
8 Maggio - 22 Maggio 2003

Boss: theguilty@hackerjournal.it

Editor: grand@hackerjournal.it,

Contributors: boymix81, CAT4R4TTA, Roberto "dec0der" Enea, Nicola D'Agostino, lele@altos.tk, {RoSwElL}, 3d0, Lidia, Il Coccia

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Immagine di copertina: Daniele Festa

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

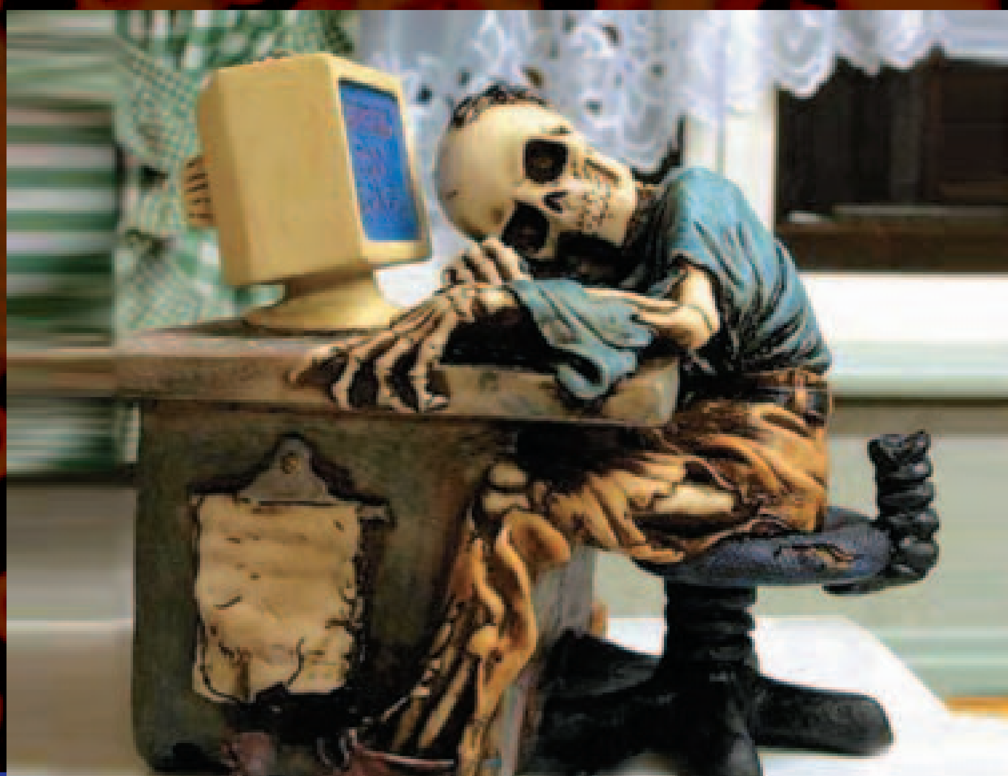
redazione@hackerjournal.it

hack'er (hãk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Smanettate di meno... e leggete di più!

grand@hackerjournal.it



www.hackerjournal.it

Saremo di nuovo in edicola Giovedì 22 maggio!



STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

E C'È ANCHE L'INSTANT (HACKER) MESSANGER



Forse i più attenti l'avranno già notato. Sulla home page del sito di Hacker Journal, in alto a sinistra, c'è un bottone chiamato Portal Messenger. Facendoci clic sopra, si vede una lista degli utenti che attualmente stanno visitando il sito (o che comunque hanno effettuato il login col proprio nickname registrato). Con un clic sul nome di un utente, si apre una finestra che permette di inviargli un messaggio immediato. Ok, non è niente in confronto alle funzionalità che si possono avere con la chat (usando il client Java del sito, o collegandosi con un normale client Irc al canale #hackerjournal di irc.azzurra.org), però è una simpatica e semplice alternativa.

I NOSTRI/VOSTRI BANNER!

Nel momento in cui scriviamo, siamo arrivati a ben 88 banner realizzati da voi e pubblicati sul sito di HJ. Ecco i più belli di questo numero:



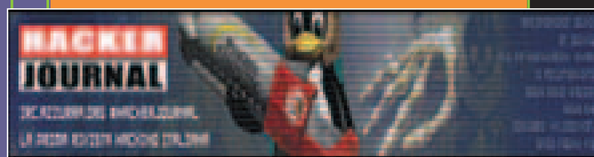
GidanMX2



Skay



Marco



{N}oRt{ON}

Dai bit alla carta



http://pcstore.altervista.org/



http://www.marcom9.tk/



www.darkweb.tk

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: cosci8

pass: bell1

GLI ARTICOLI PIÙ LETTI!

Ecco la classifica attuale dei dieci articoli più letti su **hackerjournal.it**

1. Il registro di sistema - (5785 Letture)
2. Le basi del C - (3227 Letture)
3. Eliminare CyDoor - (3090 Letture)
4. Spamming e finestre attive! - (2431 Letture)
5. anonymous - (2412 Letture)
6. CONNETTERSI CON LINUX by gaxt87 - (2288 Letture)
7. Spionaggio informatico - (2034 Letture)
8. Il Sistema Binario - (1862 Letture)
9. Try2hack la sfida continua - (1836 Letture)
10. Hacker, uno stile di vita - (1614 Letture)

HACKER JOURNAL

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

mailto:

redazione@hackerjournal.it

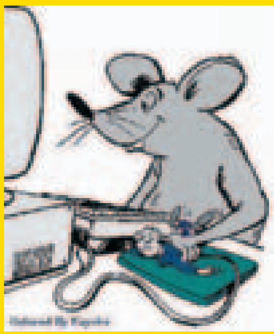
LA PASSWORD DELLE PASSWORD

Sono un po' paranoico, e utilizzo spesso la protezione dei file con password (zip, documenti di Office...). Ho impostato la password anche al Bios del mio computer. Ora tutte queste password le ho inserite in un documento di Word che ho protetto a sua volta con una password. Forse avete già intuito il problema: ho dimenticato la password del documento di Word, e quindi non riesco più ad accedere agli altri file. Ditemi che c'è una soluzione, vi prego.

Matteo M.

Non una, ma decine di soluzioni. La crittografia usata nei file di Office è – purtroppo o per fortuna – molto debole. Molto dipende dalla versione di Word utilizzata per il documento, e dal tipo di password scelta. Word 95 ha un meccanismo davvero elementare, che può essere craccato quasi istantaneamente indipendentemente dalla complessità della password. Con Word 97/2000 le cose si fanno un po' più complicate (per lo meno per quanto riguarda la password per aprire il documento; craccare la password di "sola lettura" è molto più semplice). In questo caso, se la password è una parola di senso compiuto, si possono provare attacchi di tipo "dizionario", che appunto provano tutte le parole contenute in un "dizionario" di parole. Ovviamente, il dizionario deve essere scelto in modo sensato (non usare un dizionario inglese, se sai che la tua password è una parola italiana); se la parola è compresa nel dizionario, la si può trovare nel giro di uno o due giorni con un computer di potenza media che lavora ininterrottamente. Se invece hai scelto bene la password (lettere e numeri in sequenza casuale), potrebbero volerci una o due settimane per provare tutte le combinazioni. In tutti i casi, trovi programmi adeguati (gratuiti e commerciali) all'indirizzo www.passwordcrackers.com.

☺ Tech Humor ☺



RITORNO AL DOS

Ho comprato per la prima volta il vostro giornale: fantastico! Vedo che molte cose si fanno dal prompt dei comandi, come ai vecchi tempi del dos, come potrei rinverdire questi vecchi ricordi? Come posso approfondire la mia conoscenza per interpretare meglio i vostri articoli a riguardo?

Pierlo

Se il tuo interesse è il DOS, trovi una descrizione dei comandi, molto stringata ma efficace, all'indirizzo http://windows.zdnet.it/manuali/msdos1.html. Occhio però: la maggior parte dei comandi di shell che vedi qui non sono MS-DOS, ma comandi per Linux (principalmente per la shell Bash).

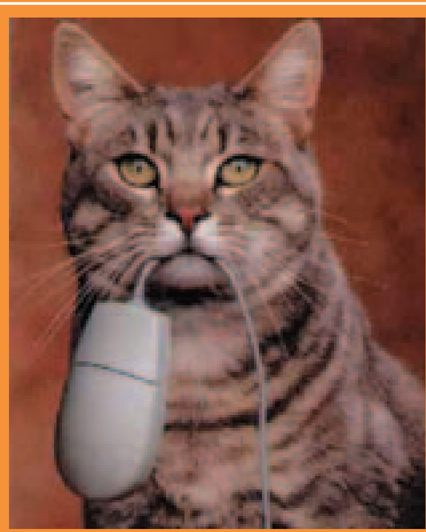
A QUALE PORTA BUSSARE

Se devo eseguire un port scanning come faccio ad individuare il numero della porta che mi interessa?

Dylan

E come faccio io a dirti qual è la porta che ti interessa? Se cerchi un servizio Ftp, la porta è la 21; se cerchi Telnet, è la 23: se stai cercando un sito Web, probabilmente è la 80. Le altre puoi trovarle nell'elenco delle "porte ben conosciute", considerate standard per i servizi Internet (anche se qualcuno potrebbe voler impostare un server Web per funzionare su una porta diversa dalla 80). L'elenco completo è su http://www.iana.org/assignments/port-numbers.

☺ Tech Humor ☺



Se invece vuoi vedere se il tuo computer ha aperta la porta caratteristica di un trojan, per eliminarlo, puoi guardare la lista presente su http://www.hackerjournal.it/php-bin/go.php?go=dbtroyan

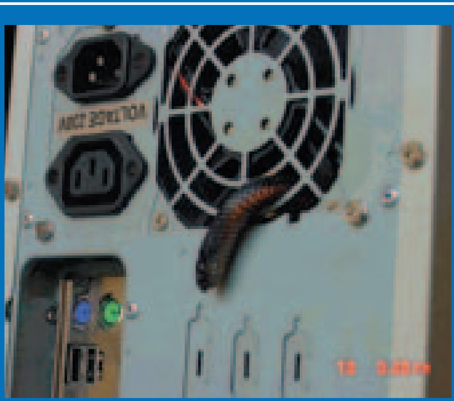
CHI CONTROLLA I CONTROLLORI?

Vorrei un chiarimento per quanto riguarda una cosa strana che mi è capitato: nel numero 10 della vostra rivista c'è un articolo (come ti spio la spia) che parla di Windows Keylogger 5.04. L'ho scaricato dal sito www.littlesister.de e quando stavo per installarlo Norton (2002) mi ha rivelato che c'erano 3 virus: keylogger.exe, Krnlmod.exe e Watchdll.dll. Sono effettivamente virus? Grazie continuate così!

Francesco

Non sono virus, però un keylogger è un programma potenzialmente dannoso e malizioso. Se

☺ Tech Humor ☺



qulacuno ti convince a installarlo a tua insaputa (magari perché è stato nascosto in un altro programma), potrebbe carpire importanti informazioni dal tuo computer. Norton sta solo cercando di fare il suo lavoro, avvisandoti dell'eventuale pericolo. Se sei sicuro di ciò che fai, puoi ignorare gli avvisi di Norton AntiVirus.

VERMI DI KAZAA

Volevo sapere se mi potevate aiutare con questo problema:
ho scaricato un file *.exe da kazaa, dopo averlo utilizzato l'ho cancellato dalla cartella condivisa di kazaa.Adesso ogni volta che accendo il compiuter nella cartella condivisa si creano files (2 ogni volta che accendo il compiuter) con estensione *.zip o *.exe nascosti con il nome di crack per vari programmi e giochi.Ho provato a lasciarli fare e dopo 4 o5 volte che accendo il c mi sono trovato tutti i miei mp3 all'interno della cartella condivisa rinominati in nome.mp3.scr.Ho provato a usare vari antivirus aggiornatissimi ma non lo ritengono un file pericoloso.Posso fidarmi che nn danneggerà il mio sistema?Come faccio a liberarmene?

Frost

A occhio e croce, ti sei preso un Worm che gira sulla rete di Kazaa, probabilmente Benjamin o Veedna. L'estensione .scr è quella degli screen saver, il cui codice viene eseguito da Windows senza verifiche sulla sicurezza da parte di alcuni antivirus (in genere quelli vecchi). Se però come dici il tuo antivirus è davvero aggiornato (ma è aggiornato solo il motore, o anche le definizioni?), dovrebbero riuscire a individuarli senza problemi. In ogni caso, prova a cercare le istruzioni per la rimozione di Benjamin e Veedna su http://securityresponse.symantec.com/avcenter/

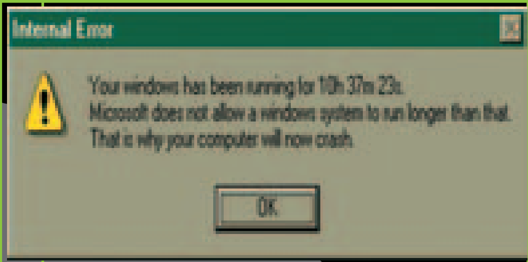
CURIOSITÀ SU VIRUS E DEFACEMENT

Sono un vostro fedele lettore e vorrei farvi 2 domande...
Sarò veloce! ;-)
A cosa si riferisce e a cosa "serve" la stringa "@MM" che c'è spesso alla fine del nome di un virus? ES: KLEZ.H@MM
Come fa ZONE-H a registrare all'istante tutti i defacement? (vengono segnalati dai Defacers o hanno un "motore particolare" che cerca tutte le pagine contenenti ad esempio: DeFaCeD By...

ZazzHack

☺ Tech Humor ☺





Alcuni produttori di antivirus (in questo caso Symantec), accanto al nome del virus mettono una sigla che identifica il tipo. In questo caso, @MM sta a indicare che il virus in questione è un "Mass Mailer", cioè un programma che si propaga inviando numerosi messaggi email. Trovi una lista delle definizioni all'indirizzo http://securityresponse.symantec.com/avcenter/vnameinfo.html
Zone-H accetta segnalazioni dai defacer stessi, che non chiedono altro che un po' di celebrità. Poco importa che quelli di Zone-H inseriscano i defacer più attivi nella pagina "Wall of Shame" (muro della vergogna); l'importante per loro è comparire, e quindi contattano Zone-H immediatamente dopo il misfatto.

☺ Tech Humor ☺



HOT!

CHIODO SCACCIA CHIODO



Pare che sia proprio "chiodo scaccia chiodo" la filosofia che anima il team di Windows Server 2003, ribattezzato lo 'scaccia-incubi', uno dei prodotti con i quali Microsoft intende 'raggiungere il punto in cui la sicurezza sia un dato di fatto e dove gli utenti utilizzino il software e le tecnologie di computing con la stessa confidenza che hanno nell'accendere una lampada o nell'alzare una cornetta del telefono'.

Gli obiettivi perseguiti da Bill Gates con il Trustworthy Computing sono il 'Secure by Design', il 'Secure by Default', ed il 'Secure by Deployment'. Con lo scaccia-incubi Microsoft si impegna a raggiungere il primo di questi obiettivi, progettando applicazioni che contengano il minor numero possibile di bug e vulnerabilità di sicurezza.

Questo più o meno dice il comunicato stampa. Noi preferiamo aspettare di verificare, con un sorriso.

HOLLYWOOD TRASLOCA SU INTERNET

Vedere film su Internet sarà presto realtà, grazie ad un accordo siglato dalle major cinematografiche di Hollywood, fondatrici del sito web Movielink.com, che consentirà di scaricare i film attraverso il sito Hollywood.com. Per usufruire del servizio è sufficiente disporre di connessioni a banda larga, mentre il costo si aggirerà tra 2,95 e 4,99 dollari a titolo.



MAILBLOCKS CONTRO LO SPAMMING



Phil Goldman, dopo anni di lavoro trascorsi nei laboratori di ricerca e sviluppo delle più importanti aziende dell'It, tra le quali Microsoft e Apple, ha deciso di 'mettersi in proprio'.

Facendo tesoro della sua esperienza di guru nel campo della protezione, Phil ha creato Mailblocks, un'azienda specializzata nella lotta allo spamming, che utilizza qualcosa di diverso dai soliti filtri.

Mailblocks (www.mailblocks.com) offre una web mail caratterizzata da un sistema di filtraggio della corrispondenza completamente nuovo, e molto originale. In pratica, qualunque mail proveniente da un indirizzo sconosciuto attiva automaticamente il filtro, che invia al mittente un form, nel quale chi ha spedito l'e-mail dovrà inserire un numero indicato nello stesso form.

Se il mittente è una persona, questa non avrà alcun problema a leggere il numero, a riscriverlo nel form, e a reinviarlo.

Se, invece, è stata inviato da un sistema automatico, il modulo di verifica non tornerà indietro e la mail verrà trattata come spazzatura.

Attendiamo speranzosi un sistema antispamming che dia meno sbattimenti dello spamming stesso..

SONY NON HA PAURA DELLA GUERRA



Mentre gran parte del mondo si è mobilitato per impedire la guerra, e si muove ora per arginarne i danni e limitarne le conseguenze disastrose, molte aziende hanno deciso di fare business sfruttando il simpatico motto "Shock and Awe", col quale l'esercito americano aveva ribattezzato l'attacco all'Iraq.

Tra queste figurava in pole position Sony, ansiosa di lanciare sul mercato un nuovo videogioco che evocasse ai giocatori momenti di gioia passata.

Bersagliata dalle critiche, Sony ha rinunciato al progetto, e si è consolata proponendo per i prossimi interventi USA "Fottili tutti" e "Caccia al brigante".

VULNERABILITÀ DEL WEB SERVER APACHE 2.0.44

IL Web Server Apache 2.0.44 è più fragile di quanto non sembri. Secondo iDefense, infatti, un attacco remoto potrebbe provocare un utilizzo eccessivo di risorse macchina da parte del demone httpd, fino al loro esaurimento. Si tratta di un errore di gestione di chunck di dimensioni consistenti, derivanti da richieste che contengono svariati caratteri di ritorno a capo (Lf, linefeed) consecutivi. Si potrebbe quindi conseguire un attacco di tipo DOS che saturi le risorse di sistema, generando semplicemente molte richieste. Il consumo di memoria diviene immediatamente molto elevato, causando un rallentamento del sistema. Oltre al modello Apache 2.0.44, secondo iDefense tutte le versioni 2.x sono vulnerabili.

LO STORAGE OLOGRAFICO È VICINO

Immagazzinare 'montagne di dati' sarà presto realtà. Si tratta dello storage olografico, che sfrutta la tridimensionalità di rilievi ed avvallamenti attraversati e letti da un raggio laser. Consente di immaganizzare molti più dati di quanto consenta un disco tradizionale, con possibilità di lettura e scrittura paragonabili a quelle di un supporto magnetico. La tecnologia prevede l'impiego di di raggi luminosi in grado di creare reazioni chimiche in un supporto nell'ambito della sua tridimensionalità.



NOKIA FA LE FUSA



Stanchi di aspettare una telefonata che non arriva mai o di lunghe chiamate di lavoro? Vibelet.com offre un'alternativa nell'uso del cellulare: si chiama Kitty, ed è in grado di rendere molto più gradevole l'uso di un telefonino. Non stiamo parlando delle solite funzioni, ma di un vero e proprio programma che trasforma il nostro Nokia in un massaggiatore, compagno ideale nelle serate solitarie o nelle lunghe attese nel traffico di città. Per saperne di più, collegatevi a www.vibelet.com/handsets.html, oppure via wap a wap.vibelet.com. Il programma funziona solo con alcuni modelli Nokia e costa 1,5 sterline inglesi.



MICROSOFT FA CILECCA DOPO 50 TENTATIVI

A chi ha installato Office 2000 SR-1 si Windows 2000, può capitare di vedere richiesta la registrazione. Nulla di strano: basta inserire i propri dati. Peccato che subito dopo averlo fatto, la richiesta compare di nuovo. E poi di nuovo, e di nuovo ancora. L'alternativa è cliccare "Register Later", ma qui si apre un'altra falla, perchè scegliendo questa opzione per più di 50 volte, se ancora non avrete scaraventato il vostro PC dalla finestra o dato fuoco alla foto di Bill Gates, Office si blocca. Tranquilli però: Microsoft non solo ammette l'esistenza del problema, ma ha la soluzione! Il divertimento continua infatti con una procedura di 23 passi che comporta nientemeno che la modifica del registro di configurazione di Windows. Nell'indicare la soluzione, Microsoft ci ricorda comunque che usare l'Editor del Registro di configurazione può essere molto pericoloso e possiamo farlo a nostro rischio e pericolo. Non saranno delle cime a scrivere programmi, ma a Redmond hanno un gran senso dell'umorismo.

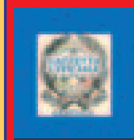


HOT!

TISCALI FA ACQUA

Si moltiplicano in questo periodo le proteste contro l'ADSL Tiscali su gruppi di discussione, forum di Tiscali ecc. Pare infatti che, a causa di disservizi Tiscali, gli utenti Tiscali stiano diventando parecchio nervosi. vigare. Un lettore di Hacker Journal, Festus, ha aperto un sito dedicato (http://tiscaliadsl.da.ru) che raccoglie sempre più consensi. Andate a vedervelo e dite la vostra.

SOLDI PER NIENTE



Il decreto legislativo sul diritto d'autore è stato definitivamente approvato e pubblicato sulla Gazzetta Ufficiale, ed entrerà in vigore come legge dello Stato dal prossimo 29 aprile 2003.
Sulla base di questa legge saranno applicati i seguenti sovrapprezzi anche ai supporti vergini, cioè ai dischi dove non è memorizzato nulla, tantomeno prodotti dell'ingegno di una artista: 0,29 Euro per ora di registrazione per minidisc, CD-R audio e CD-RW audio; 0,23 Euro per 650 megabyte per CD-R dati e CD-RW dati; 0,36 Euro per 64 megabyte per flash memory e MP3; 0,87 Euro per 4,7 GB per DVD Ram, DVD-R e DVD-RW.

I CRACKER ATTACCANO BOTTONE

K.C.Hatcher, di San Francisco, è partita per qualche giorno di vacanza, ed al suo rientro si è vista recapitare una bolletta telefonica di 12.000 dollari, per telefonate mai fatte! Pare che qualche idiota si sia divertito ad utilizzare la linea telefonica della povera Hatcher per qualche breve ed innocua chiamata personale. Come? Semplice, bypassando la password della sua segreteria telefonica. AT&T e SBC Communications, operatori della linea interessata, non tutelano i loro utenti dagli idioti, e in questo caso si sono limitati ad applicare uno sconto del 35% sulla bolletta. Quindi occhio a codici di accesso e password, che possono rivelarsi un boomerang pericoloso non solo su PC e Bancomat, ma anche su normalissime segreterie telefoniche.

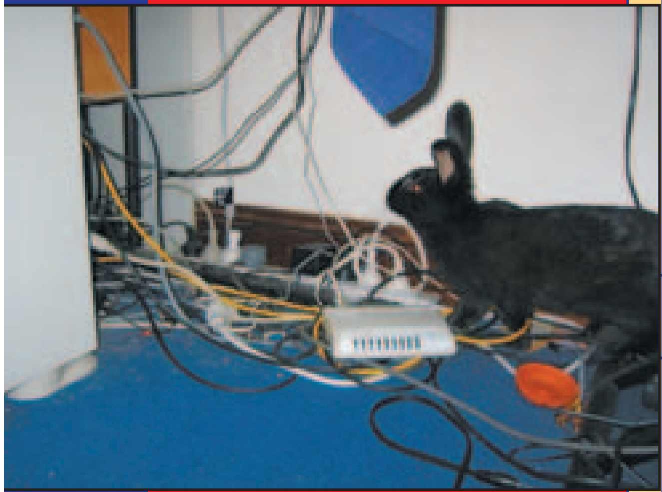
HOT!

MAGLIETTE VOLANTI



Per anni abbiamo cercato di tirare avanti sentendone la mancanza, ma finalmente l'attesa è finita... con il "Tee Launcher" possiamo lanciare t-shirt ad una distanza di circa 50 metri! L'apparecchio è ricaricabile in pochi secondi, facilissimo da usare, e spara t-shirt, ma anche fiori, muffins, hot dogs, palline di gomma, palloncini, o qualunque altro oggetto non pesante e non troppo fragile. Il costo dell'arnese, comprensivo di accessori, è di 1.400 dollari, e ormai non c'è un solo organizzatore di concerti rock che non ne abbia uno in dotazione.

OCCHIO AL CONIGLIO



I conigli sembrano animali piuttosto mansueti, ma quelli con la passione per i computer possono giocarci brutti scherzi. Fatevi un giro su http://home.iprimus.com.au/cojoco/Naughty_Bunny.html, e guardate cos'è successo ad ad un poveraccio che ha trovato un coniglio in un parcheggio, se l'è portato a casa, gli ha dato da mangiare, e dopo qualche giorno ha scoperto che nel menù del piccolo ospite c'erano anche cavetti e microchip del suo computer!

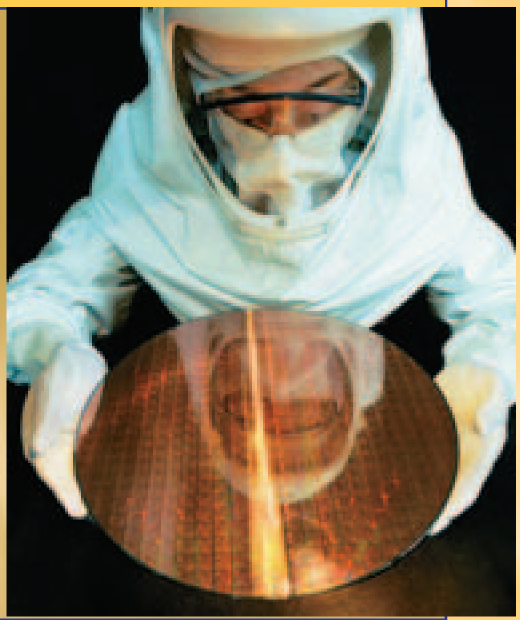
IBOX FA LARGO A IPOD

Dopo il progetto di clonare un Mac con l'iBox, adesso qualcuno ha deciso di ispirarsi parecchio al famoso lettore portatile Apple di MP3 iPod. Samsung, per esempio, ha annunciato in questi giorni il lancio di un nuovo MP3 portatile che assomiglia parecchio al gioellino di Apple. Si chiama Yepp YP-55, e sarà il primo MP3 portatile con Dolby Sorround. Un prodotto simile è Bantam's BA1000: grande come l'iPod, è dotato di una memoria da 2 GB a 5 GB, può contenere fino a 1.800 canzoni, ha cinque modalità di equalizzazione predefinite (rock, jazz, classical, pop, custom), 32 MB SDRAM, ed è compatibile con qualunque PC



3 GIGAHERTZ DI PAURA

Dopo il ritardo nel produrre i suoi processori, AMD stava davvero stappando una bottiglia del migliore champagne alla notizia che anche Intel era messa male con il suo superprocessore da 3 Gigahertz, che friggeva più in fretta di un uovo piazzato nel microonde. Purtroppo per AMD, però, e per la gioia di tanti produttori che aspettavano solo i 3 Gigahertz per vendere nuovi computer alle folle assetate di velocità, pare che il problema del nuovo Pentium 4 sia molto meno grave di quanto non si pensasse, e che il ritardo effettivo sia limitato a una settimana. Intel ha quindi ripreso a consegnare il suo più veloce processore Pentium, insieme a una patch software, e a sfornarne a ciclo continuo, con la sua ben nota destrezza. Per contrattaccare, AMD ha pronta una sorpresina che dovrebbe farle guadagnare molto nel settore dei server aziendali, regno indiscusso del sua acerrimo rivale.



REALNETWORKS HA FATTO LA SPESA

Sembra proprio che in RealNetworks siano diventati improvvisamente parecchio ottimisti. Non si spiega, altrimenti, la decisione di spendere la bella somma di 36 milioni di dollari per comprarsi Listen.com, la società che gestisce il servizio Rhapsody di ascolto di musica via Internet e di creazione di CD musicali con brani



scelti dall'utente. RealNetworks, dopo aver chiuso un 2002 in netta perdita e aver fatto diversi sacrifici, aveva già investito un bel po' di quattrini in Listen.com, e con l'acquisizione si gioca davvero molto. Chi usa RealPlayer per ascoltare musica e radio o per vedere filmati via Internet si catturi una bella schermata adesso che sembra piuttosto in salute, non garantiamo nulla per i prossimi mesi.

LO STRUMENTO PRINCIPALE PER DIVENTARE HACKER: LA TESTA

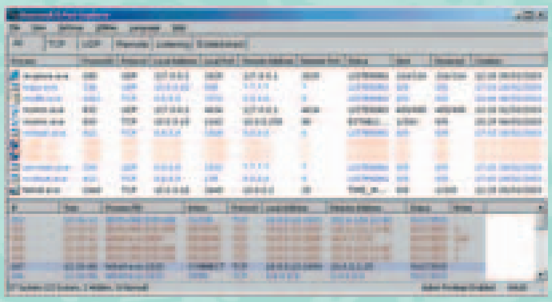


I FERRI DEL MESTIERE

Ogni hacker si sceglie un certo numero di programmi che poi usa con passione e magari riscrive addirittura di suo pugno. Vediamo un po' come funzionano e dove si trovano alcuni degli strumenti più usati.

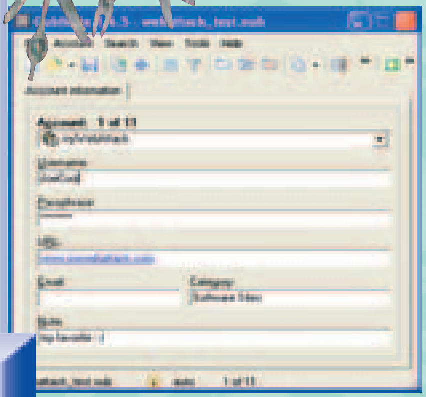
Port Explorer

Sapere tutto, ma proprio tutto, su qualsiasi stringa di dati di tracciare un pacchetto per vedere che percorso compie e quanto si ferma presso ciascun server. Il sito da cui scaricare questo gioiellino è http://www.diamondcs.com.au/portexplorer/, dopo aver provato per un mese



transiti attraverso le porte del nostro computer è davvero difficile. Port Explorer è in grado di fornirci queste informazioni e di fare altre simpatiche cose come localizzare geograficamente la sorgente di una trasmissione dati o il programma, possiamo decidere di pagare circa 30 dollari alla DiamondCS per averne la licenza d'uso. Tra tutti i modi che ci sono per spendere 30 dollari in Rete, questo potrebbe rivelarsi uno dei più fruttuosi.

Oubliette



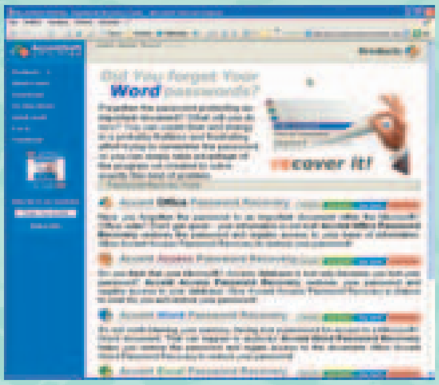
Le password devono essere: difficili da indovinare, complicate da scrivere, con numeri e lettere maiuscole e minuscole e possibilmente con qualche carattere ASCII non digitabile da tastiera. Visto che poi non bisogna mai scriverle da nessuna parte, prima o poi rischiamo di trovarci tagliati fuori dalla nostra posta elettronica o, peggio ancora, dal nostro computer, ed essere costretti a passare ore a craccare i nostri stessi file. Per evitare questa imbarazzante quanto inconfessabile situazione, Oubliette si offre di ricordare per noi le nostre password e di conservarle al riparo da occhi indiscreti. Logicamente anche Oubliette ha una password, e se ci dimentichiamo quella è il disastro più totale, però almeno lo sforzo mnemonico è alla portata anche di chi ha poco tempo e tanti account. Oubliette è gratis e si può scaricare da http://www.tranglos.com/free/. Il programma è Open Source e, se ci divertiamo a programmare, possiamo personalizzarlo come vogliamo.



LO STRUMENTO PRINCIPALE PER DIVENTARE HACKER: LA TESTA

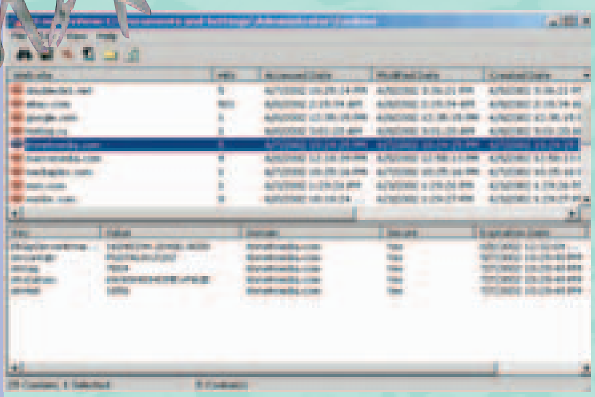


Password Recovery Tools

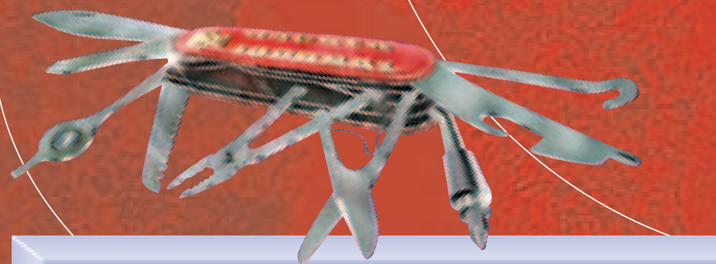


Qualcuno si è davvero specializzato nel recuperare password dimenticate, cosa che gli rende senza dubbio onore. Se abbiamo problemi con una password di un qualsiasi documento di Office, facciamo un salto su http://www.passwordrecoverytools.com/, ci sono programmi di recupero password specifici per ogni applicazione.

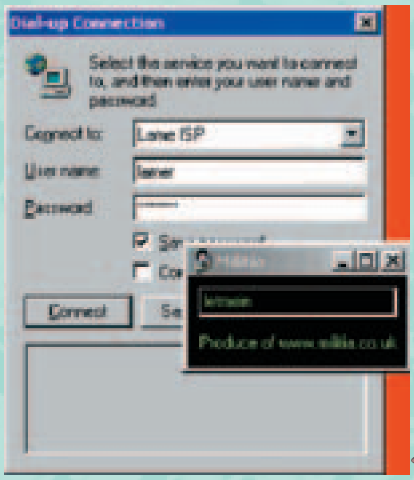
IECookiesView v.1.50



A cancellare tutti i cookie sono capaci in molti, ma aprirli, modificarli e selezionarli per farne quel che vogliamo è molto più divertente e utile. IECookieView è un piccolo programma gratuito che ci permette di fare questo e altro interagendo alla perfezione con Internet Explorer. Se abbiamo accesso ad altri computer attraverso la rete, IECookieView ci permette di aprire e modificare i cookie presenti su macchine remote e di salvare negli appunti il contenuto di questi file. Scarichiamoci subito la versione 1.50 di questo pratico strumento collegandoci al sito http://nirsoft.tripod.com/. Una sola piccola raccomandazione: se non amiamo i popup, attiviamo un programma di protezione dalle fastidiose finestrelle prima di andare sul sito di IECookie; il suo autore ci tiene a lasciare freeware il programma, ma in compenso crede che i nostri monitor possano ospitare più finestre di un megacondominio.

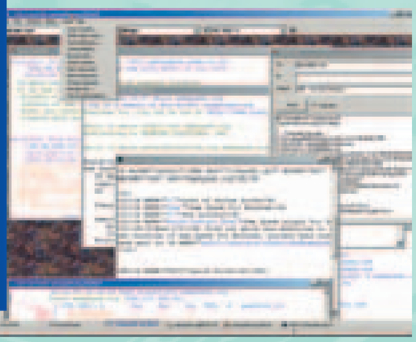


Militia Password Revealer



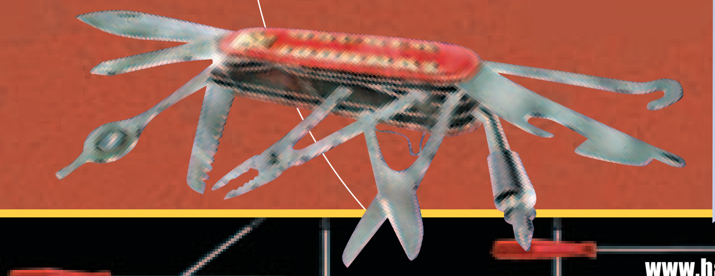
Dal sito http://www.militia.co.uk/ possiamo scaricare uno dei più semplici ed efficaci programmi per recuperare password da box di testo. Militia Password Revealer è gratuito, come altre due o tre stranezze che si trovano in questo sito.

Sam Spade



Questo programma sta a ogni navigatore esperto come un coltellino svizzero sta a uno scout: senza non si può andare avanti.

Sam Spade comprende numerosi moduli di controllo del traffico in Rete, di verifica dei server, traceroute, finger, whois e via dicendo. Dal sito http://www.samspade.org/ssw/download.html possiamo scaricare questo gratuito e utilissimo pacchetto software, mentre se vogliamo divertirci un po' senza installare nulla, già che ci siamo, facciamo un salto su http://www.samspade.org/t/.

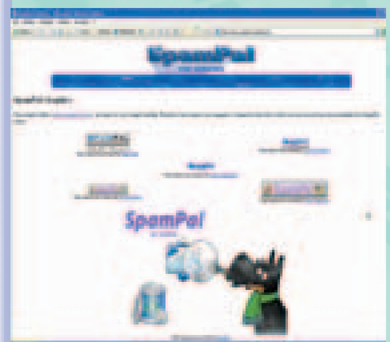


Cloak 6.0



La steganografia è una tecnica davvero interessante, per quanto ci siano alcuni limiti che deve ancora superare. Il programma Cloak 6.0, disponibile in versione demo al sito http://www.insight-concepts.com/. Per quanto il suo funzionamento sia identico a molti altri programmi, Cloak ha un aspetto estremamente curato e pure il sito sembra fatto decisamente bene. Gli esteti della crittazione sanno cosa scegliere.

SpamPal



Se lo spamming è un problema, una prima difesa può arrivare proprio da SpamPal, che è gratis, piccolo e semplicissimo. Lo troviamo al sito http://www.spampal.org/ e l'unica cosa che dobbiamo fare con attenzione una volta scaricato e installato il programma è configurarlo. Se lo addestriamo bene, questo piccolo eseguibile ci proteggerà dai più grossi rompiscatole della rete, se regolato male, invece, SpamPal può considerare spazzatura messaggi che invece vorremmo leggere, come quello della solita Natasha che impazzisce per noi un giorno si e uno no.

Purge IE 5.01

Piccolo, leggero ed efficace, Purge IE funziona come uno scopino da passare sulle nostre orme per evitare che qualsiasi persona che accede al nostro computer possa capire cosa abbiamo fatto su Internet. Il programma si può scaricare da http://www.purgeie.com/, si può usare per 15 volte e poi bisogna pagare circa 20 dollari. La versione Pro è un po' più ricca di funzioni, però costa dieci dollari in più.



Email Express

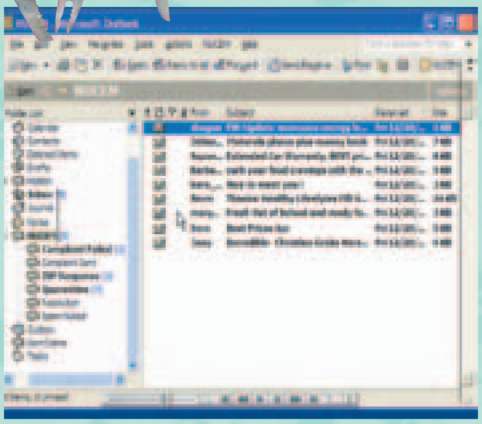


Molto più ricco di funzioni, ma gratuito solo per i primi 60 giorni è Email Express. La versione Pro, uscita da poco, è altamente configurabile e può soddisfare le esigenze della maggior parte degli utilizzatori della Rete. Nessun programma antispam è infallibile, ma questo funziona proprio bene. Le liste di spammer vengono aggiornate di frequente e sono facilmente modificabili anche a mano. Il sito di Privacy Labs, ben organizzato e piuttosto veloce, è all'indirizzo http://www.privacylabs.net. facciamoci un salto anche se non ci interessa Email Express, ci sono un paio di programmini freeware che meritano di essere scaricati.

Tiny Personal Firewall

Un firewall software è in grado di tenere alla larga dal nostro computer la maggior parte dei rompiscatole che si aggirano su Internet. Tiny Personal Firewall è sempre stato gratis, ma dall'arrivo della versione 4.5 è diventato come molti altri: si può provare per 30 giorni e poi bisogna comprarselo. Per quanto questo cambiamento sia scocciante, capiamo benissimo quelli di Tiny software, al sito http://www.tinysoftware.com/. Questo è un programma eccellente e robusto, e loro devono pure campare.

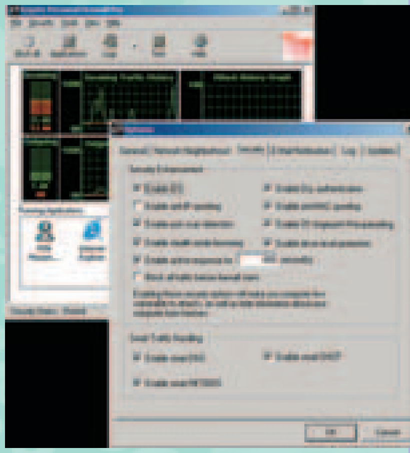
Nucem 2.0



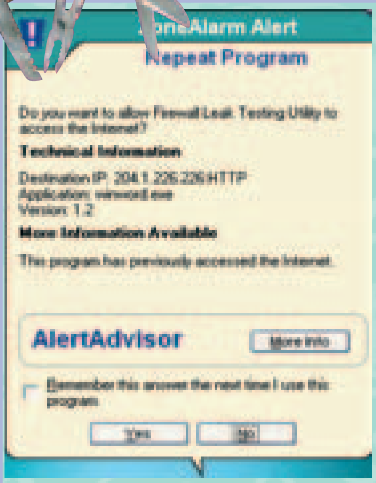
Veloce, semplice, pratico e nemmeno caro. Si chiama Nucem 2.0 e molti di noi lo hanno provato con una certa soddisfazione. Resta sempre il problema che, non si capisce perché, se un'americana che impazzisce per noi vuole chiederci di telefonarle o di andare a vedere il suo sito a pagamento Nucem 2.0 la blocca subito, ma per il resto il programma non è male. Il sito per scaricare la demo è http://www.helpmesoft.com/.

Sygate firewall

Dal sito http://soho.sygate.com/ possiamo, anzi dobbiamo, scaricare uno dei migliori programmi firewall in circolazione. Dobbiamo farlo non solo perché proteggere le nostre macchine e impedire a un cracker di sfruttarne la potenza elaborativa è un dovere, ma anche perché Sygate offre il suo firewall gratis per uso personale. Il firewall di Sygate è tra i pochi, insieme a Zone Alarm, che è stato capace di non farsi fregare da LeakTest, un geniale eseguibile del quale parliamo più avanti che ha messo in ginocchio BlackIce e altri blasonati firewall.

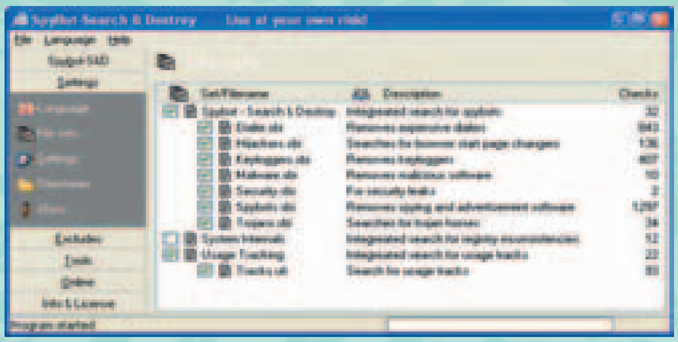


Zone Alarm



Zone Alarm è il firewall software più famoso e uno dei più sicuri. Molti lo usano con soddisfazione da anni e lo si può scaricare gratis da http://www.zonelabs.com. La protezione offerta dalla versione base è accettabile, quella della versione Pro invece è eccellente, con la possibilità di regolare diversi parametri e di autorizzare operazioni e programmi uno per uno. Sempre Zone Labs produce uno degli strumenti più amati da molti nostri conoscenti: Steganos Security Suite 4. Se avete qualcosa da nascondere, questo è il pacchetto che fa per voi.

Spybot Search and Destroy

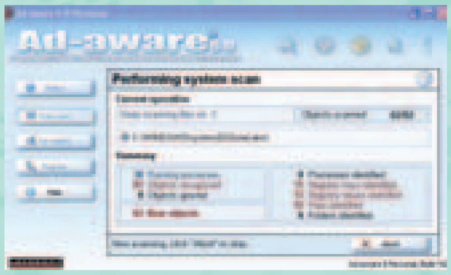


La steganografia è una tecnica davvero interessante, per quanto ci siano alcuni limiti che deve ancora superare. Il programma Cloak 6.0, disponibile in versione demo al sito http://www.insight-concepts.com/. Per quanto il suo funzionamento sia identico a molti altri programmi, Cloak ha un aspetto estremamente curato e pure il sito sembra fatto decisamente bene. Gli esteti della crittazione sanno cosa scegliere.

Popup Zero Pro

Quando si naviga su Internet, c'è sempre il rischio di imbattersi in qualche sito che si è venduto l'anima al diavolo in cambio di cinquemila finestre che devono aprirsi sullo schermo di ogni visitatore. Se a noi i popup non sono mai piaciuti, avere questo programma può migliorarci la vita. Le finestre che sbucano dal nulla non ci sono più, guardiamo solo i siti che ci interessano e non foraggiamo un sistema di pubblicità invadente e odioso. Possiamo scaricare Popup Zero Pro da http://www.pcssafe.com/ e usarlo per un mese, poi dobbiamo pagare poco meno di 20 dollari per la licenza. Dallo stesso sito possiamo scaricare anche Tracks Eraser XP, un pratico strumento per coprire le tracce che lasciamo navigando in Rete.

Ad-Aware

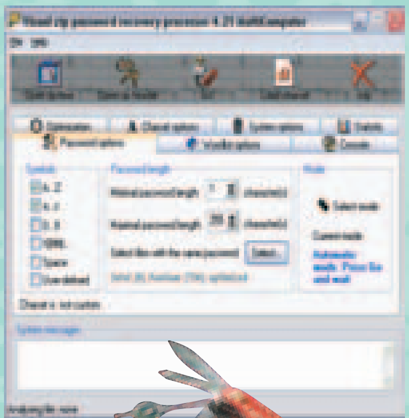


Il programma più famoso e più usato per togliere di mezzo spyware e altre fastidiose bestiole ha un nome: Ad-Aware. Le versioni che si possono scaricare da http://www.lavasoft.de/ vanno da quella gratuita, che cerca ed elimina i programmi spioni che si intrufolano nel computer, fino a quella Professional, che costa quasi 40 dollari ma che blocca anche i popup, i tentativi di dirottare il browser durante la navigazione e le aree di memoria che contengono dati sensibili. Tutti quelli che usano il computer con una certa serietà hanno installato almeno la versione freeware, anche perché farsi spiare da sconosciuti è una delle cose meno divertenti che si possano fare in Rete.

Password Recovery XP

Scordarsi una password a volte può essere drammatico, e più siamo stati attenti a scegliere qualcosa di difficile da indovinare, più sarà dura ricordare che razza di combinazione avevamo scelto. Password Recovery XP, di iOpus, fa quasi impressione: tira fuori le password di Windows come se fossero già in un file di testo... Il programma si può prelevare da http://www.iopus.com e, nello stesso sito, troviamo anche il fratellino minore (e gratuito) di Password Recovery: 123 Write All Stored Passwords (WASP) V2.01. Questo piccolo programma permette di recuperare rapidamente tutte le password memorizzate nell'archivio di Windows.

Visual Zip Password Recovery Processor 4.7



Un programma che si vanta di eludere il 90% delle password a protezione di archivi zippati in 60 minuti è piuttosto invitante, se poi mantiene la promessa è da non perdere. Scaricatelo da http://www.zipcure.com/ e iniziate subito a mettere alla prova le vostre password: ne vedrete delle belle. Il programma si può provare per un mese ma poi bisogna pagare circa 30 dollari per la licenza.

Vita facile: una suite



Per chi ha un po' di soldi spendere (bene), o magari ha una piccola azienda e preferisce avere "solo software originale" consiglio di prendere in considerazione l'acquisto di Tiger Suite 4.0 (69 $!). È una vera e propria raccolta di programmi che funzionano piuttosto bene e forniscono in un colpo solo tutto ciò che serve per analizzare e migliorare la sicurezza del proprio sistema e della rete. Sono così tante le sue funzioni che non ci è possibile elencarle qui per problemi di spazio, ma potete trovarle al sito www.tigertools.net.

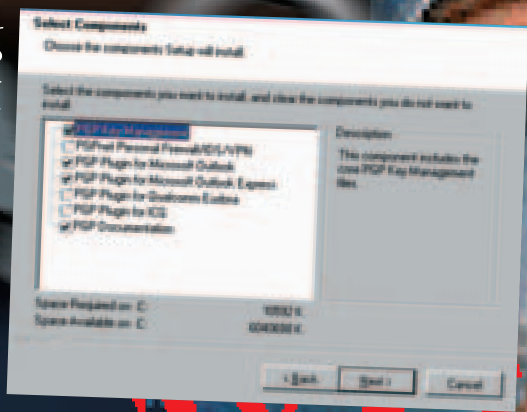
I VOSTRI DOCUMENTI TOP SECRET

PGPPERS

AVETE MAI AVUTO LA SENSAZIONE CHE QUALCUNO UNA DELLE RISPOSTE POSSIBILE È

Volete essere sicuri che l'appuntamento al buio con la vostra amante non diventi al contrario una serata di profondo rosso dove la vostra fidanzata urla come una pazza per casa inseguendovi con un bastone? Bene, se desiderate che questi quadretti di vita restino solo all'interno del piccolo schermo forse quello che fa per voi è il software **PGP Personal 8.0**.

Sia le aziende che i privati hanno spesso il bisogno di sapere che i dati in transito nel network e quelli presenti all'interno del loro computer siano sicuri da occhi indiscreti; quale mezzo migliore per giungere al risultato se non quello di "nascondere" i files in questione? Abbiamo parlato nel numero scorso di Invisible Secret, un programma che serve appunto a nascondere i file e le cartelle agli occhi indiscreti. Questa volta prendiamo in esame un programma che invece di nascondere fisicamente un file agli occhi di eventuali curiosi in modo che non sia rintracciabile cercherà di nascondere il contenuto del file stesso rendendolo indecifrabile.



COSA CONTIENE

PGP Personal 8.0 racchiude una suite di due prodotti: **PGP Mail** e **PGP Disk**. E' una suite da utente singolo, a pagamento, che garantisce la protezione totale del vostro computer. PGP Mail gestisce la posta elettronica, sia da un punto di vista di e-mail, sia come protezione di allegati, inoltre gestisce anche il criptaggio dei messaggi immediati per coloro i quali usano ICQ o MSN. Inoltre incorpora in sé la gestione delle chiavi PGP sia come creazione che come mantenimento. PGP Disk gestisce invece il disco o i dischi rigidi, proteggendo i files contenuti al loro interno.



PGP è senza dubbio il prodotto più completo sul mercato, e basa la sua forza essenzialmente sulle seguenti caratteristiche:

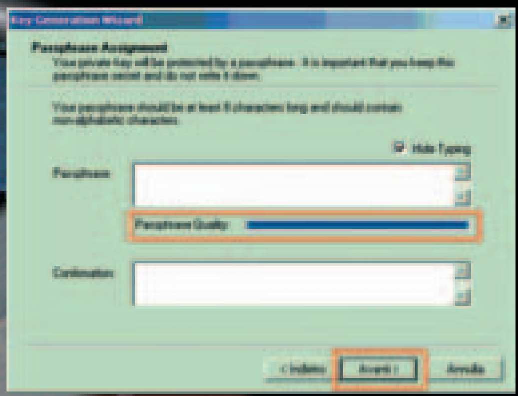
- Criptaggio dei dati con chiavi simmetriche a 128 bit
- Adattabilità sia al singolo utente che alle aziende
- Sviluppo di tools che permettono l'impostazione di politiche precise e configurazioni adatte ad ogni singola situazione
- Interoperabilità fra i vari algoritmi di criptaggio
- Compatibilità fra più piattaforme e più client e-mail: tutte le versioni di windows dal 95 a XP, sistemi Mac, Windows CE e Palm OS



NEWBIE

ONAL 8.0

SPIASSE I VOSTRI DATI O LEGGESSE LE VOSTRE MAIL?
QUELLA DI CIFRARE I PROPRI DATI.



ASSICURIAMOCI LA POSTA

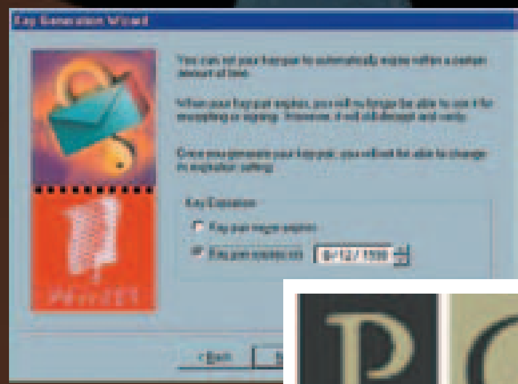
PGP Mail unisce le caratteristiche di criptaggio dei dati e la possibilità di utilizzare firme digitali in modo da rendere sicuri i vostri dati e da garantire che i vostri messaggi non saranno letti da nessun'altra persona se non quella cui è diretta la e-mail. La possibilità, inoltre, di utilizzare firme digitali fa si che l'identità del mittente sia assicurata e testimonia il fatto che la mail non è stata contraffatta nel transito.
PGP Mail supporta, come abbiamo visto in precedenza, numerose piattaforme e numerosi client email; nello specifico i client di posta adattabili all'uso sono:

- Microsoft Outlook 97, 98, 2000 e Outlook XP
- Microsoft Outlook Express 4.x e 5.x

Tutti questi client di posta possono essere impostati sia come POP3 che come IMAP

...E IL DISCO

PGP Disk è un tool che permette la creazione di dischi col contenuto interamente criptato. Come è ovvio può essere utilizzato su qualunque piattaforma, ma gli autori ne consigliano l'utilizzo soprattutto nei sistemi portatili data la maggiore facilità con cui questi possono essere rubati o persi. L'utilizzo di questo software mette invece al riparo da ogni possibile perdita di dati. L'interfaccia molto intuitiva e creata con una seri di wizard che si susseguono, fanno sì che il processo di creazione della chiavi, come quello di mantenimento e di azione sui viri files, sia semplificato al massimo non creando alcun tipo di problema anche per gli utenti meno esperti. Il programma può essere eseguito automaticamente all'avvio oppure solo nel momento in cui necessitiamo dell'accesso ai files.



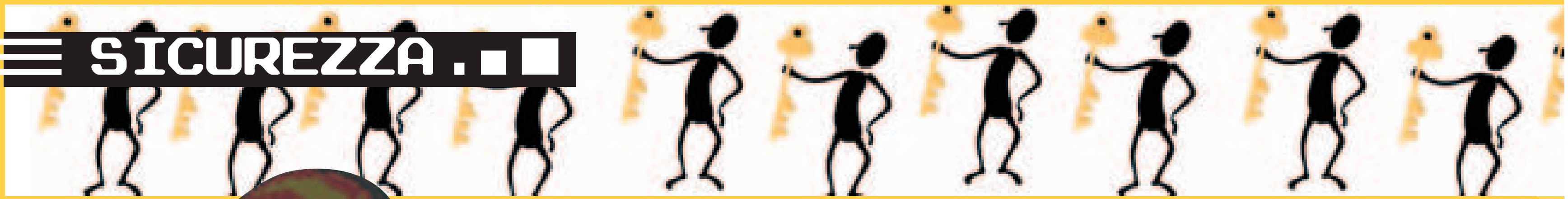


PGP Personal 8.0 supporta i seguenti sistemi operativi:

- Windows XP
- Windows 2000
- Windows NT
- Windows ME
- Windows 98SE
- Windows 98

Come abbiamo detto sono supportati anche i sistemi operativi Palm OS; al momento della stesura di questo articolo però l'ultima versione per questa piattaforma non è stata ancora rilasciata, quindi l'istallazione di PGP Personal 8.0 fa perdere la capacità di sincronizzazione delle chiavi col palmare. Ricordiamo inoltre che sono supportate numerose varianti di Smart-Card ed altri supporti di sicurezza tipo PKCS#11.

CAT4R4TTA, cat4r4tta@hackerjournal.it



COME FUNZIONANO LE CHIAVI HARDWARE PER LA PROTEZIONE DEI SOFTWARE



SOFTWARE BLINDATI

Spesso i programmi più costosi non possono essere eseguiti senza che nel computer sia inserita una chiave hardware di protezione. Ma per ogni nuovo sistema di protezione, possono esistere contromisure efficaci.



Sebbene oggi si senta sempre più spesso parlare di modelli di business connessi con la filosofia dell'open source molti programmatori hanno ancora la necessità di tutelare il proprio business con **metodi tradizionali che scoraggino la duplicazione abusiva di materiale coperto da copyright**.

Qualcuno ricorderà l'utilizzo dei cosiddetti "dischi chiave" ovvero dei supporti magnetici opportunamente alterati in fabbrica che non permettevano la copia del media attraverso programmi di duplicazione come il diskcopy ed altre utilità analoghe. O forse, sarebbe stato più corretto dire che **non avrebbero dovuto permettere la copia**. Sistemi di questo genere sfruttavano l'incapacità di molti programmi di copiare da dischetti danneggiati su determinate tracce, che però lo erano solo dal punto di vista logico e non fisico.

Tali protezioni però erano molto blande, poichè bastava talvolta utilizzare un'accoppiata diversa di hardware e software (come molti copiatori per Amiga) per poter bypassare questa limitazione ed avere una copia funzionante del programma originale.

Oggi però molte cose sono cambiate e ormai nessuno più (si spera) proteggerebbe le proprie creazioni con strumenti così poco validi. Ecco allora che **sono entrate in gioco tecnologie molto più sofisticate e che si basano su microchip che integrano una logica crittografica** e che permettono di ottenere risultati molto soddisfacenti sotto vari fronti: le chiavi hardware (dette in gergo dongle).

L'accoppiata "chiave hardware" e "software protetto" è un binomio vincente da qualche anno a oggi. Malgrado qualsiasi informatico sappia benissimo che **nessun sistema possa essere inattaccabile sotto ogni fronte**, può comunque ragionevolmente affermare che una protezione del genere è una via percorribile per varie ragioni.

La validità di tali strumenti hardware, infatti, è oggi fuori discussione visto che implementazioni ibride hardware-software sono in uso anche in token per l'autenticazione degli utenti e per lo scambio di password e credenziali di rete.

>> Servizi offerti

Malgrado sul mercato esistano numerose dongle, tutte offrono le stesse principali caratteristiche:

- Protezione dalla copia
- Crittografia del codice eseguibile
- Crittografia della base di dati
- Resistenza ad attacchi di reverse-engineering

Tali servizi sono forniti dall' "intelligenza" del motore crittografico contenuto molto spesso in **una piccola chiave da inserire nella porta USB o in quella Parallela**, e che costantemente comunica con il driver preposto alla crittografia e decrittografia di dati e programmi e che, **in mancanza della chiave originale, non permette al software di venire eseguito** e dunque di fatto la copia illegale viene inibita, perché produrrebbe un programma inutilizzabile.







senza la presenza del della dongle. La protezione dal reverse-engineering viene fornita su molti fronti:

- cifratura/decifratura a run-time dell'eseguibile
- Verifica della presenza della chiave
- Routine anti-debugging

La prima funzionalità viene fornita da **una parte di codice chiamata envelope**, che rende il programma eseguibile nel solo momento del caricamento in memoria, facendolo rimanere protetto e cifrato quando è salvato su disco. Le varie utility di disassembly **non possono dunque far trapelare nulla per ciò che riguarda il codice**, visto che le varie istruzioni in linguaggio macchina sono cifrate e quindi intelligibili solo al momento del caricamento in memoria. La sicurezza, però non si ferma qui, visto che si potrebbero effettuare **attacchi sulle routine di cifratura / decifratura** (in chiaro) che devono essere per forza presenti per la corretta esecuzione del programma protetto. Ecco allora che si affianca all'envelope, la **possibilità di personalizzare delle proprie chiamate di interrogazione alla chiave hardware,** che sono particolarmente difficili da individuare e rimuovere. Infine, altre funzioni per l'intercettazione di eventuali debugger in esecuzione completano il quadro della sicurezza globale.



>> Limiti del sistema

A questo punto ci si potrà allora chiedere quali siano i limiti di questi strumenti che a prima vista offrono una protezione così completa e robusta.
Come accennato precedentemente, **in informatica non soltanto non esistono strumenti sicuri al 100% ma anzi i sistemi di sicurezza possono essere attaccati sotto vari fronti.**
Bisogna infatti chiedersi il come tutti questi meccanismi si realizzino, in pratica, sia nel software che nell'hardware e come essi vengano implementati di fatto in un sistema operativo moderno.
Partendo dagli attacchi hardware, **è possibile ottenere una copia di tali chiavi con degli strumenti alla sola portata di aziende di semiconduttori**, sebbene vi siano anche centri specializzati nella duplicazione di chiavi hardware (anche e soprattutto dei vecchi modelli).
L'oggetto "chiave hardware" viene duplicato letteralmente trattandolo come "scatola nera" alla quale, vengono applicati degli opportuni segnali ed ai quali reagisce con predeterminati segnali in uscita.
Dal lato software, invece, c'è da dire che **attacchi condotti con successo su tutti i tipi di protezione ci sono stati e ci sono**, specie nei confronti di programmi professionali e dal costo molto elevato. E' comunque importante dal lato dei programmatori sottolineare che anche il modello implementativo dei driver gioca un ruolo fondamentale nella protezione del parco software.
Infatti, proprio per garantire una compatibilità con tutti i tool di sviluppo le varie dongle vengono corredate da librerie software sotto forma oltre che di driver anche di DLL, ActiveX e quant'altro possa essere richiamato facilmente da qualsivoglia eseguibile. **Questo fatto comporta però una potenziale falla di sicurezza**, nel senso che **è molto più facile intercettare una chiamata ad una DLL** (magari sostituendo la stessa DLL con una costruita ad hoc) che replicare le funzionalità di un driver di sistema. In conclusione, però è opportuno ribadire l'efficacia nella maggioranza dei casi in cui lo sviluppatore adotti una dongle per programmi costruiti ad hoc per aziende e privati, dove è sicuramente più conveniente l'acquisto della licenza che un paziente lavoro di reversing!

Paolo Iorio



QUALI UTILITY E COMANDI DA TERMINALE È BENE CONOSCERE E USARE

OTTIMIZZARE MAC OS X



Pulizia del disco, miglioramento delle prestazioni: viaggio tra falsi miti e veri problemi.

Come abbiamo visto nell'articolo precedente OSX è un mix molto particolare di novità, solide basi UNIX e della tradizione dei precedenti MacOS. Quando si tratta di tenere "sotto controllo" il sistema e fare un po' di pulizia gli utenti hanno a che fare con una situazione spesso complessa ed è necessario destreggiarsi tra potenziali problemi, operazioni utili, e altre un po' meno.

>>E' tempo di... fare pulizie

Un caso in cui Darwin/OSX si dimostra in tutto e per tutto un OS di tipo UNIX è quello di **programmi che vengono eseguiti automaticamente dal sistema intervalli regolari,** ad esempio di notte, quando il carico di lavoro della macchina è minore. Questi programmi vengono supervisionati e lanciati dal comando **'cron'** e solitamente indicati nel file **'/etc/crontab'**.
Un buon esempio sono i tre script:

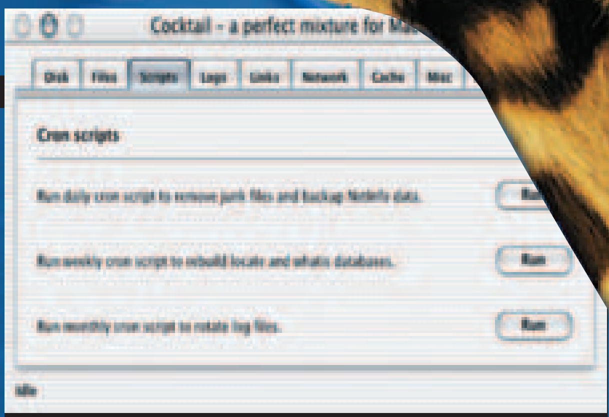
```
/etc/daily
/etc/weekly
/etc/monthly
```

la cui esecuzione è eseguita con cadenza giornaliera, settimanale e mensile, rispettivamente.
Questi svolgono una moltitudine di compiti utili: **cancellazione di vecchi file temporanei, generazione di statistiche, ricostruzione dei database, copie di backup** ed altro ancora.
Il problema è l'orario di esecuzione che è in genere notturno. Laddove su un server questo non rappresenta un problema (è acceso 24 ore su 24), lo è invece sulle macchine desktop, spente o messe in stop (sleep) alla fine della giornata lavorativa.
La soluzione è far eseguire manualmente i comandi via terminale. Digitando

```
sudo /etc/daily
```

seguito dal tasto invio verrà chiesta la password di amministratore e verrà eseguita la procedura. Lo stesso va fatto con sudo /etc/weekly e infine con sudo /etc/monthly
Alternativamente si può usare un tool multiuso come **Cocktail** (www.dicom.se) o meglio ancora utility ad hoc come **anacron** (disponibile tramite il gestore di pacchetti software Fink, http://fink.sourceforge.net) che provvederanno ad eseguire automaticamente gli script alla prima occasione, solitamente all'avvio.





Cocktail è un pacchetto di utility per l'ottimizzazione di Mac OS X.

>> Eliminare i file .DS_store

Non è solo la parte UNIX a necessitare di pulizie: anche il lato che attiene a funzioni proprie del Mac necessita di qualche cura, soprattutto quando si scambiano file con il mondo Windows o Linux. Precisamente, **a "sporcare in giro", è il modo in cui OSX gestisce tutte le informazioni aggiuntive sui file nelle cartelle**.

Qualche numero fa (HJ #17) abbiamo parlato dei Desktop Files in MacOS, che, nascosti, contengono informazioni utili alla macchina ma potenzialmente molto pericolose per la privacy quando fatte girare, ad esempio su un CD masterizzato, fuori dal proprio Mac.

OSX ha invece **i file ".DS_Store", creati dal Finder in ogni directory per "tenere a mente" una serie di informazioni** come posizione e dimensioni delle finestre, icone, commenti. Come visto nella scorsa puntata il punto davanti al nome serve a rendere invisibile il file, almeno agli utenti comuni. Tutti gli altri possono usare un "**ls -la**" da Terminale o l'utility freeware **Tinker Tool** (www.bresink.de/osx/TinkerTool.html).

Il problema dei file .DS_Store è che **ce ne sono a migliaia in tutto il sistema** dato che ogni directory ne ha uno e che quando si masterizzano CD, si fa ftp o si scambiano dati con macchine Windows o Linux (ad esempio in una rete mista via Samba) o più semplicemente si riavvia e usa il Mac con OS9, **i file in questione possono comparire in bella vista**.

A livello di privacy **il problema è meno grave di quello relativo ai file DesktopDB di Mac OS 9,** ma comunque è poco carino perché, **oltre ad essere uno sgradevole inestetismo, dai .DS_Store file si può ricavare ad esempio un elenco dei file presenti nella directory** (per esempio i documenti o i programmi installati), cose che gradiremmo restassero comunque private e confinate entro i limiti del nostro hard disk.

Per l'eliminazione di questi file le soluzioni sono varie e riconducibili a due approcci.

La prima è **usare dei programmi ad hoc, come De_DDS** (www.extraneous.us/download/De_DDS.tgz), **DS_Store Cleaner** (www.ryangrier.com/projects/ds_store_cleaner/), **Clean Up smb mess 1.1** (www.faqintosh.com/risorse/as/AS_cleansmbmess.sit) o il costoso (e corredato di pacchiana iconografia) **DS_StoreTerminator** (www.reservoirmedia.com/dst.html).

Meglio ancora è impiegare il Terminale e una combinazione di efficaci utility da shell. Digitando:

```
sudo find /Volumes/nome-
deldisco -name .DS_Store -
print0 | xargs -0 rm
```

verranno rimossi tutti i .DS_Store sul disco o partizione "nomedeldisco" (ovviamente da sostituire con il nome del vostro hard disk).

Sotto OSX 10.2 (Jaguar) è possibile usare anche

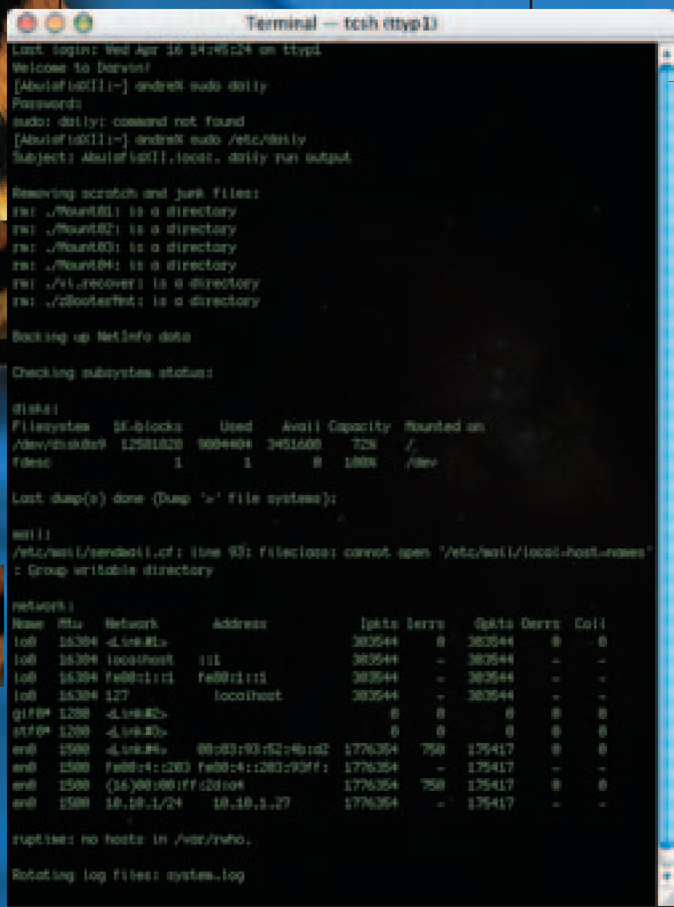
```
sudo find /Volumes/nome-
deldisco -name .DS_Store -
delete
```

Oppure altre combinazioni a scelta dei comandi "find", "grep" e "rm".

Nota bene: i programmi e i comandi da Terminale vanno eseguiti solo sul disco o sulla cartella specifica che si vuole condividere o copiare. **Farlo altrove è inutile, e anzi resetterebbe molte impostazioni utili**. Si raccomanda inoltre che il disco o la cartella in questione non siano aperti nel Finder nel momento della ripulitura, né che vengano riaperti dopo, perché il Finder **ricreerà al volo il file .DS_Store e saremmo punto e a capo**.

>> Il "mito" dell'update prebinding

Sotto OSX esiste un meccanismo chiamato "prebinding". Molti avranno notato che quando si installano certi programmi (succede spesso con gli aggiornamenti Apple) c'è una fase alla fine denominata "**Optimizing System**" o qualcosa del genere. Si tratta appunto del "prebinding" che serve ad **accellerare l'apertura dei programmi installati.**



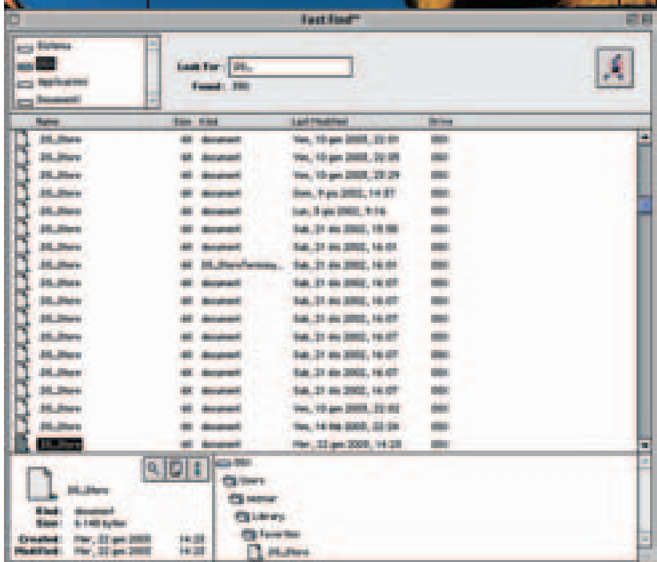
Alcuni script di manutenzione sono programmati per essere eseguiti di notte, ma se il computer non è acceso, non entreranno mai in funzione. Si pososno attivare manualmente dal Terminale, oppure con utility ad hoc.

QUALI UTILITY E COMANDI DA TERMINALE È BENE CONOSCERE E USARE

In MacOSX **i programmi non sono composti da un unico file ma da numerosi pezzi sparsi**, che vengono cercati, usati e caricati all'occorrenza, tra cui le librerie, alcune delle quali fornite da Apple stessa. Le librerie possono venire aggiornate aggiungendo nuove funzioni, motivo per cui si usa questa tecnica, detta "dynamic linking" (invece del "direct linking" che crea un unico amalgama inscindibile) che tiene le librerie slegate dai programmi veri e propri. La modularità ha però un costo in termini di performance e allora **il prebinding si incarica di "fissare" questo collegamento rendendo il caricamento delle librerie più rapido**. Per questo motivo si è diffusa l'abitudine tra gli utenti di rifare ogni tanto il prebinding "a mano" per rendere il sistema più efficiente (per esempio dopo aver installato nuovi programmi) .
Il comando usato è:

```
update_prebinding -root
```

Altri comandi relativi al prebinding ma più specifici sono "**fix_prebinding**" e "**redo_prebinding**" di cui si possono avere le spiegazioni grazie al manuale in linea scrivendo nel Terminale:
`man nomecomando`



Mac OS X registra alcune informazioni utili in file chiamati .DS_Store, invisibili in OS X, ma visibilissimi (e piuttosto noiosi) in ogni altro sistema (Mac OS Classico compreso).

Per chi invece preferisce evitare i comandi da shell ci sono diversi programmi che effettuano questa (cosiddetta) ottimizzazione, a partire dal già citato Cocktail. Tra gli altri ci sono **Xoptimize** (www.tonbrand.nl/page1.htm#HTML_Optimizer), **SpeedMeUp Pro** www.nonamescriptware.com), **Mox Optimize** (http://users.skynet.be/cefs/alex/vente/mox2) e **Maintain1 X** (http://mirror.macupdate.com/info.php/id/7380).
Ma torniamo al prebinding: negli ultimi anni, come dimostra anche la pletora di utility scritte all'uopo, **si è diffusa la convinzione che questa operazione aiutasse notevolmente OSX**, che era nelle vecchie versioni tutt'altro che "scattante". In realtà non solo **pare che il prebinding abbia un'incidenza molto limitata sulla reattività del sistema** ma **dalla versione 10.2 non è più necessario** in quanto è l'OS stesso ad eseguirlo quando installa aggiornamenti e programmi.
Attenzione quindi a non cadere nell'effetto placebo e usare a tutti i costi questa tecnica (che anzi alla lunga può mettere a dura prova il disco fisso) per cercare di spremere di più il proprio Mac.

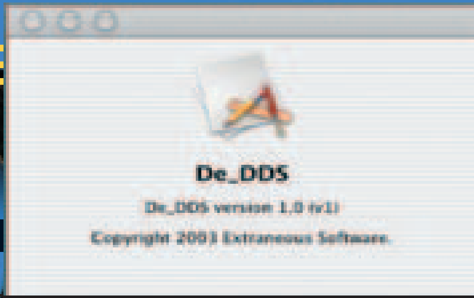
>> Copiare file Mac "classici"

Anche se sotto OSX c'è un sistema BSD, il filesystem consigliato (fortemente consigliato) per l'uso è il classico HFS+ che mantiene l'integrità e la coesione di **molti file Mac tuttora composti da due parti strettamente interconnesse: data fork e resource fork.**
Lo stesso vale nel caso di copia o di archiviazione e compressione dei file mac "classici": un semplice trascinamento su un volume formattato UFS o un disco Windows o l'uso del comando "tar" da Terminale **rovinerebbe irrimediabilmente vecchi font, programmi e suoni e farebbe perdere informazioni preziose ad immagini e altri documenti.**
Per ovviare è **necessario usare strumenti specifici**: uno di questi è il noto programma di compressione standard StuffIt, che nella versione completa (quella a pagamento) per OSX funziona addirittura anche da linea di comando.
Altre soluzioni sono copiare o comprimere usando da Terminale l'utility "**ditto**" con impostata l'opzione specifica "**-rsrcFork**" (così da usare il formato AppleDouble su filesystem che non supportano i resource fork)

```
ditto -rsrcFork nomedelfile destinazione
```

oppure possiamo optare per altre **versioni modificate da Apple dei comandi da shell**. Invece di "cp" e "mv" bisogna usare "**CpMac**" e "**MvMac**" e invece dell'archiviatore "**tar**" si usa "**hfstar**".
Un'ultima nota: molte di queste funzioni sono disponibili solo installando i "Developer Tools", preziosissima fonte di informazioni e applicativi per lo sviluppo e sopratutto per lo smanettamento.
I Developer Tools sono allegati come CD addizionale con OSX o disponibili da scaricare gratuitamente sul sito Apple previa registrazione (http://developer.apple.com/tools/).

Nicola D'Agostino
dagostino@nezmar.com



DS Terminator e DeDDS sono utility che rimuovono i file .DS_Store lasciati in giro su volumi di rete o dischi rimovibili.

PER APPROFONDIMENTI...

Jepson B., Rothman e., Mac OS X for Unix Geeks, 2003 O'Reilly
ISBN 0-596-00356-0

Prebinding Explained
What is prebinding and when does it need to updated?
http://radio.weblogs.com/0100490/stories/2002/08/24/prebindingExplained.html

Apple Developer Connection
http://developer.apple.com/





UN URL CHE È TUTTO UN PROGRAMMA...

Prendi il controllo del tuo browser, facendogli eseguire i Javascript che decidi tu!

Prima di addentrarci nell'argomento di questo articolo, faccio una triste considerazione. **La maggior parte degli utenti di Internet non ha mai usato la funzionalità di Bookmark** (o Preferiti) del proprio browser, e magari non ha mai modificato la home page preimpostata. Se però avete questa rivi-



sta tra le mani, **probabilmente questo non è il vostro caso** e, anzi, vorrete cavare qualcosa di più dal vostro strumento di navigazione. Partiamo allora.

>> Non tutto il Javascript vien per nuocere

Spesso, il linguaggio Javascript **viene usato nelle pagine Web per annoiare fino alla morte i navigatori di un sito**. Finestre che si aprono sullo schermo, o che cambiano di forma e dimensione; scritte che scorrono nella barra di stato (impedendo la visualizzazione di informazioni, queste sì, utili). Imparandolo un po' (o "rubando" in giro del codice già fatto), **è però possibile fare eseguire al proprio browser le istruzioni Javascript di propria scelta**. Per esempio, si può creare uno script che apra una finestra sullo schermo, con un form nel quale inserire una parola da trovare sul Web col proprio motore di ricerca preferito. Oppure modificare le dimensioni della pagina con misure di propria scelta. Le possibilità sono tante. Una volta capito che con Javascript possiamo prendere il controllo del browser **rimane da capire dove inserire questo codice**. Una pagina da salvare in locale? Magari da impostare come home page? Nah! In alcuni casi può funzionare, ma in generale è meglio trovare una posizione sempre accessibile, indipendentemente dalla pagina che si sta visitando.

>> Il colpo di genio

Pensa che ti ripensa, qualcuno ha intuito che molti script Javascript, per essere eseguiti, non hanno bisogno di risiedere in una pagina. **Possono benissimo essere inseriti nella barra dell'indirizzo**, con la sintassi **javascript:script da eseguire**. Ve lo immaginate però che noia dover inserire ogni volta uno script a mano? Ma, ricordate l'inizio dell'articolo? **I bookmark sono lì apposta per evitarci di inserire a mano gli indirizzi Web**. Ecco la soluzione: creare dei bookmark che, invece di un indirizzo, contengano il listato di un programmino Javascript. Ecce Bookmarklet.

>> Bookmarklet per tutti

Sul sito www.boorkmarklets.com si possono trovare mini script per tutti i gusti. Da semplici finestrelle che permettono di **cercare un testo** (inserito in un form o selezionato nella pagina) con i principali motori di ricerca, a quelle che permettono di **caricare l'indirizzo successivo o precedente di una serie di pagine numerate** (utile se volete vedere tutte le immagini da www.sitoporcello.com/pr0n/foto1.jpg a www.sitoporcello.com/pr0n/foto2543.jpg); dagli script che fanno **scorrere la pagina verso il basso** a intervalli predefiniti di tempo, a quelli che **ridimensionano la pagina, o modificano il colore di sfondo e del testo**. Ce n'è davvero per tutti, ma attenzione. A causa delle differenti implementazioni di Javascript da parte di Netscape Navigator ("inventore" del Javascript) e di Internet Explorer (Microsoft, basta la parola...), **moltissime bookmarklet che funzionano con uno, non vanno sull'altro browser**.





La RETE è fatta a SCALE...

...e ogni pacchetto di dati, per giungere a destinazione, deve attraversare vari livelli. Approfondiamo un po' il modello OSI, che abbiamo citato nei numeri scorsi.

>> Livello 7: Applicazione

È il livello più alto del modello OSI, **interagisce con l'utente e tratta direttamente le applicazioni** (application program interface). Nel livello 7 risiedono il SO di rete e tutte le altre applicazioni quali posta elettronica, condivisione file, gestione database, etc etc.
Gli standard di questo layer sono **SAA** (System Application Architecture) di IBM e anche **X.400 Message Handling**. Come abbiamo già detto questo è probabilmente il livello più importante, o per lo meno il più evidente, poiché in diretto contatto con l'utente.

7- APPLICATION	applicazione
6- PRESENTATION	presentazione
5- SESSION	sessione
4- TRANSPORT	trasporto
3 -NETWORK	rete
2 -DATA LINK	colleg dati
1 -PHYSICAL	fisico

I LIVELLI DEL MODELLO OSI/ISO

Qui vedete l'ordine dei sette livelli del modello OSI/ISO.

>> Livello 6: Presentazione

Questo livello riguarda riguarda il **formato dati e ha la capacità di gestire i formati speciali e la crittografia.** Oltre a questo, qui risiedono anche i codici di controllo, set caratteri e loro funzioni grafiche. Anche il protocollo HTTP (per "formattare" le pagine web) è un protocollo tipico appartenente a questo livello.
Capita anche che i sistemi operativi di rete usino codifiche diverse, tipo EBCDIC oppure ASCII. In poche parole il livello sei di presentazione serve per l'interpretazione dei dati da parte del ricevente.

>> Livello 5: Sessione

Anche questo livello è molto importante perché **permette a due applicazioni (o alle sue parti) di comunicare attraverso la rete** per eseguire azioni che riguardano la sicurezza e tutta l' amministrazione.

>> Livello 4: Trasporto

A questo quarto livello, come si può capire dal nome, è delegato il compito del trasporto dati. Infatti, si occupa di **fornire un trasferimento dati sufficientemente affidabile**, correggendo anche gli eventuali errori. Fraziona tutti i messaggi in pacchetti, controlla il loro ordine e i loro errori.
Questo quarto livello viene chiamato anche "end-to-end" perché è il primo che **agisce indipendentemente dalla tipologia di rete sulla quale è situato**. I protocolli principali di questo livello sono **TCP** (Transmission Control Protocol) e UDP (User Datagram Protocol). Il TCP si occupa della scomposizione e ricomposizione dei dati, ma anche di controllarli, infatti, gli eventuali dati danneggiati o persi vengono ritrasmessi. **L'UDP** invece non esegue alcun controllo.

>> Livello 3: Rete

Il livello 3, chiamato anche "Network", **si occupa del percorso che devono fare tutti i pacchetti dati**, cioè indica la vera e propria "strada fisica". Diciamo che ci sono due elementi hardware fondamentali: per primi gli switch che filtrano e direzionano il traffico, quindi i pacchetti dati e le schede di rete che li formatta, tanto da renderli "riconoscibili" e in un certo senso compatibili con i programmi che hanno il compito di direzionarli.
Questo terzo livello **utilizza maggiormente il protocollo IP**, difatti il 90% delle reti dispone di questo protocollo per l'indirizzamento e comunque tutta la gestione dei pacchetti viaggianti in rete (e anche per la definizione di indirizzi). Il protocollo IP inoltre, viene usato anche nel livello transport, quindi nel quarto.

>> Livello 2: Collegamento dati

Questo livello gestisce il flusso dati fra i vari sistemi e indica come collegare tra di loro i caratteri in modo da formare il messaggio, inoltre li analizza e li controlla prima del loro invio.
Utilizza vari protocolli, quali: **BSC (Binary Sinchronous Communications Protocol), ADCCP (Advanced Data Communications Control Procedures) e HDLC (Hight-Level Data Link Control)** e vari altri. Quest'ultimi servono semplicemente per dirigere i messaggi verso la giusta direzione e a verificare che siano stati effettivamente ricevuti.
Per apprendere meglio, tutto questo procedimento può essere paragonato a quello analogo del protocollo FTP, che individua gli errori e ritrasmette i dati durante lo scambio dei file.

ISO/OSI	TCP/IP
Application	
Presentation	Application
Session	
Transport	Transport
Network	Internet
Data Link	Network
Physical	Interface

Ecco qua la relazione tra i livelli OSI/ISO e quelli TCP/IP. Potete notare una certa somiglianza.

>> Livello 1: Fisico

Finalmente siamo arrivati al level one! Dal nome capiamo già che **si occupa totalmente della parte fisica della trasmissione dati, cioè hardware**. Infatti i cavi coassiali, le fibre ottiche, le schede ethernet... sono elementi fondamentali di questo livello. Gli standard sono stati decisi da ISO, ma anche da CCITT.
Ognuno di questi livelli, interagisce pienamente con quello sotto. Ciò significa che Applicazione interagisce con Presentazione, Presentazione con Sessione, e cosi via. È meglio dire "riceve dati" al posto di interagire, appunto perché, per funzionare, il modello OSI permette lo scambio dei dati da un livello a l'altro (sempre rispettando l'ordine del successivo), per poi arrivare all'ultimo, quindi livello fisico. Questo livello fisico passa i dati al livello fisico dell'altro host, che provvederà poi a passare il tutto al livello superiore (e cosi continua il ciclo).
Ai dati, ogni volta che passano da un livello all'altro, viene aggiunta una piccola intestazione, ma non possono essere modificati.

>> In campo TCP/IP

La suddivisione in livelli del modello OSI può essere paragonata alla suddivisione del protocollo TCP/IP suite. Infatti la suddivisione è simile (figura2).

Livello Application: nel TCP/IP non esistono i livelli sessione e presentation, infatti dopo il transport troviamo direttamente l'application, contenente tutti i protocolli di alto livello, per esempio (quelli prima introdotti e ora i più usati): Telnet, SMTP, FTP, NNTP, DNS e infine HTTP.

Livello Transport: si occupa della qualità del servizio che offre, quindi il trasporto dei dati, correggendo gli errori. Qui, come nel modello OSI, troviamo due protocolli: TCP e UDP.
Con il TCP, di connessione, tutti i dati arrivano nel giusto modo. Spezzetta inoltre il flusso dati e li manda al layer sottostante, quindi al livello Internet. L'UDP (User Datagram Protocol), non è un protocollo di connessione, quindi per niente affidabile, visto che i pacchetti possono arrivare in modo "disordinato" o addirittura non arrivare.

Livello Internet: il protocollo di questo livello è l'IP, che si occupa del routing, quindi del direzionamento dei pacchetti. Il compito di questo livello è far viaggiare i pacchetti, in modo da farli giungere a destinazione, anche se magari in un pc di un'altra rete.

Livello Network Interface: ecco l'ultimo livello della suite TCP/IP, chiamato anche "host-to-network layer" poiché invia pacchetti IP nella rete. Qui non esiste un modello fisico, in quanto si usano piattaforme hw, comunque conformi agli standard IEEE 802.

7	Application	SMB, NCP e FTP
6	Presentation	CP
5	Session	Nessuno Prot
4	Transport	TCP, SPX, NWLink, NetBEUI
3	Network	IP, IPX, DLC DecNET, NetBEUI
2	Data Link	Solo lo standard IEEE 802
1	Physical	Solo lo standard IEEE 802

Qui vedete i protocolli usati dai vari livelli.

>> I vantaggi dell'OSI

La suddivisone in livelli della gestione di una rete, quindi del modello OSI, comporta dei vantaggi:
innanzitutto riduce la complessità, grazie alla divisione in livelli stessa, poi standardizza le interfacce o i componenti, facilita la creazione dei componenti (quindi sia software che hardware), assicura l'interoperabilità, quindi consente una gestione indipendente dal tipo di piattaforma (sia hw che sw) e infine velocizza lo sviluppo perché permette l'implementazione di ogni livello indipendentemente da un altro.

Federico Lagni, azzurra #sistemisti

HACKER JOURNAL

Guestbook!

“Che sistema operativo usi e perché lo hai scelto?”

Non pensavamo che la domanda sul sistema operativo generasse tante risposte così accalorate, e così diverse tra loro! Quindi spostiamo di un numero i risultati sul futuro possibile della Rete, proponendovi le ultime risposte del domandone sul Sis. Op.

Uso solo linux, la libeta e una cosa di tutti, come linux (dany9) • Io uso Linux per imparare e uso windows perkè sbagliando si impara! (Cyph3r) • Il ststema operativo che uso e WXP, per la copatibiltà con gli altri, ma per chi come ME che ha la possibilità di avere un secondo disco fisso –e un cassetto estraibile– in questo ci installa un bel LINUX, sopratutto per imparare (SP1D3RN3T) • Io uso windows. Non importa che windows sia, io dico solo che con opportune modifiche windows è molto meglio di linux o altri fidatevi. (Andreaforever2001) • Uso Mac OS perché preferisco usare il computer per fare qualcosa d’altro, e non passare il tempo a cercare di farlo funzionare (Gianni) • Mac OS X: la semplicità di Windows con la potenza di Unix! (Josi) • Io ho Windows XP e l’ho scelto per la sua personalizzazione,ma credo che l’unico S.O. riuscito bene a Microsoft sia Win98 (Electro) • Io uso Windows ME, perche’ lo ritengo il migliore, a parte XP (Electro) • Volevo solo dire che mi stanno sul **** tutti quelli che dicono “ winzozz, linux è meglio,…” xke’ lo dicono solo x farsi vedere.Nonostante cio’ NON SONO ASSOLUTAMENTE CONTRARIO A LINUX! (Deeder) • Uso 2 sistemi operativi: Linux (debian 3.0 o red hat 8) e windows (xp)..mi piacerebbe lasciare windows ma il lavoro non me lo consente. ^_^ (zylux) • Io uso Windows XP, l’ho scelto perchè mi piacerebbe carpirne le potenzialità e imparare a capire quali sono i suoi punti deboli, a scopo preventivo inerente la mia sicurezza (Max) • Io uso sia windows ke linux perchÃ© credo ke insieme lavorino molto meglio ke staccati (manuel86) • Purtroppo io utilizzo windows e il bello è che non so il perchè...so solo che dovrei cambiare perchè non sopporto quando mi segnala MEMORIA INSUFFICIENTE PER ESEGUIRE L’OPERAZIONE quando ho aperto solo il Notepad! (gibooone) • winXp: per i giochi nn se ne può fare a meno :-/ Linux: è meglio di win, sono un curioso e credo nell’opensource. FreeBSD: tanto per provare e fare incazzare un po’ di più bill gates (UnoStrano) • Amiga naturalmente, perchè fa cio che vuoi, e SOLO QUELLO! Opzionalmente uso Linux, ma sempre su Ami per l’abbondanza del software! Altre porcherie di pseudo sistemi operativi fanno quello che fa comodo ai produttori e ogni tanto quando non si bloccano permettono di giocare (Massimo) • OS X della Apple perche è l’UNIX più facile che ci sia (Sandro) • Io utilizzo Micro$oft Windows 2000 professional per tre semplici motivi: stabile, completo, masterizzato (Net’s Angel - OverNET Crew) • Io dalla disperazione provai a farmelo uno, ma mi sono fermato al boot in protected mode :o/ (wormkill) • Fino a due anni fa usavo AmigaOS 3.9, un OS snello e facile da usare , dove anche il più inesperto poteva mettere mani senza fare cazzate. Da quando si è rotto l’Amiga , purtroppo, uso Windows XP e AmigaOS sotto emulazione. Il perchè di Win è presto detto. E’ il SO più utilizzato e ci si trova di tutto , ma non riesco ad abbandonare il mio AOS 3.9 (Nicola Lanese)

Sul prossimo numero!

La domanda a cui rispondere, con una decina di parole, è:

“Dialer, spamming, pubblicità invasiva: Internet libera esiste ancora?”

Mandate le risposte a: guestbook@hackerjournal.it

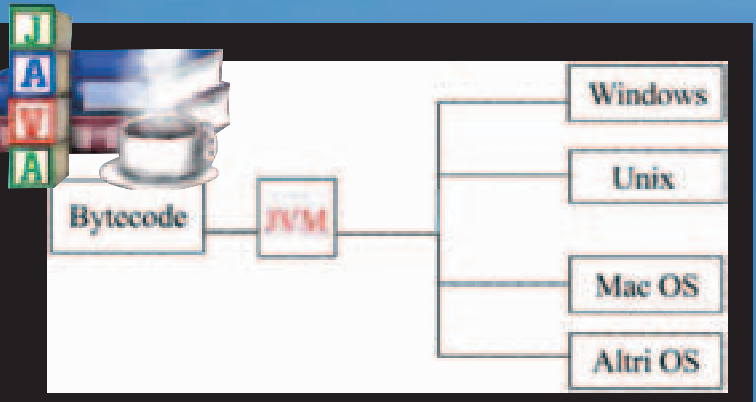
Java

Un linguaggio universale che funziona su ogni piattaforma.

Il linguaggio di programmazione Java nasce nei primi anni '90 nei laboratori di ricerca di Sun Microsystems. L'intento iniziale dei ricercatori della Sun era quello di **creare un linguaggio che non dipendesse dall'hardware e che servisse per facilitare lo sviluppo di software integrato in dispositivi elettronici**, come ad esempio il videoregistratore o la lavatrice. Il nome iniziale di questo progetto fu Oak, che poi per questioni di Copyright venne abbandonato in favore di Java . Si narra che il nome derivi da una marca di caffè che i ricercatori bevevano nel periodo di progettazione di questa nuova tecnologia. La prima versione definitiva del prodotto, il Java Development Kit, vede la luce nel 1995 e noi, a pochi anni di distanza, andremo a gustarci tutte le potenzialità che si celano dietro Java 2.

>> I vantaggi di Java

Come abbiamo avuto modo di sottolineare, la caratteristica che sta decretando il successo di Java consiste nella **totale portabilità del codice** da noi scritto. Questo significa che **non è necessario ricompilare il codice sorgente sulla macchina in cui vogliamo giri un programma scritto in Java**. Il bytecode, ovvero il codice Java che **viene interpretato ed eseguito dalla JVM (Java Virtual Machine)**, può essere portato da un sistema all'altro senza modificare nessuna riga di codice, purché sul sistema sia presente il software in grado di interpretare il bytecode. La JVM è appunto un apposito ambiente di runtime che si occupa dell'interpretazione ed esecuzione del bytecode. Java quindi è un linguaggio di programmazione sia compilato che interpretato. La compilazione del sorgente, il codice che noi possiamo scrivere utilizzando un semplice editor di testo, **dà origine al bytecode che in seguito verrà interpretato dalla Java Virtual Machine** (fig.1). La presenza di questo ambiente di runtime, inoltre, garantisce una sicurezza nella stesura del codice che difficilmente si ha con un altro linguaggio di programmazione. Infatti **la Macchina Virtuale controlla ogni operazione effettuata rendendo impossibile l'utilizzo della memoria in maniera illecita**. Ovviamente anche Java presenta delle pecche che portano spesso alcuni programmatori ad utilizzare altri linguaggi. L'esistenza della JVM, che si frappone come un muro tra il software e l'architettura del nostro Sistema Operativo, rende **impossibile la scrittura di software che si interfacci con l'hardware**. La creazione di un driver per il nostro modem, ci porta quindi ad utilizzare altri linguaggi di programmazione, come il C o meglio ancora l'Assembly. Ancora, la dipendenza del bytecode dalla JVM, porta ad un **calo delle prestazioni e questo lo si avverte maggiormente in calcolatori un pò datati**. Questi svantaggi non devono comunque farci dimenticare che la tecnologia Java sta rivoluzionando il mondo della programmazione. Ricordiamo che Java è un linguaggio multipiattaforma, e questo di fatto abbatte le frontiere poste dall'architettura dei diversi sistemi operativi. Un'applicazione scritta ed eseguita su Windows potrà girare



La Java Virtual Machine interpreta il bytecode e permette ad un software di girare su qualsiasi piattaforma.

tranquillamente anche su Linux, senza modificare una riga di codice. Sun per riassumere le potenzialità di Java dice: "Write once, run everywhere", ovvero, **"scrivi una volta, esegui ovunque"**… Possiamo darle torto?

>> Variabili e tipi di dati

Quando si affronta lo studio di un nuovo linguaggio di programmazione è buona norma andare a vedere **quali sono le regole sintattiche che ci consentono di scrivere codice in modo corretto**. Ogni programma deve potere manipolare dati che verranno inseriti in apposite strutture: le variabili. In Java per definire una variabile usiamo il costrutto tipo identificatore = inizializzazione. Per esempio:

```
int numero = 10;
```

L'inizializzazione consiste nell' assegnare un valore al tipo di variabile che abbiamo appena definito. Questa può avvenire anche in un secondo momento:

```
int numero;
numero = 10;
```

Oltre alle variabili abbiamo le costanti, che differiscono dalle prime perché il valore che gli assegniamo non può essere mutato. Per definire una costante aggiungiamo la parola chiave "final" prima di definire il tipo:

```
final int NUMERO = 10;
```

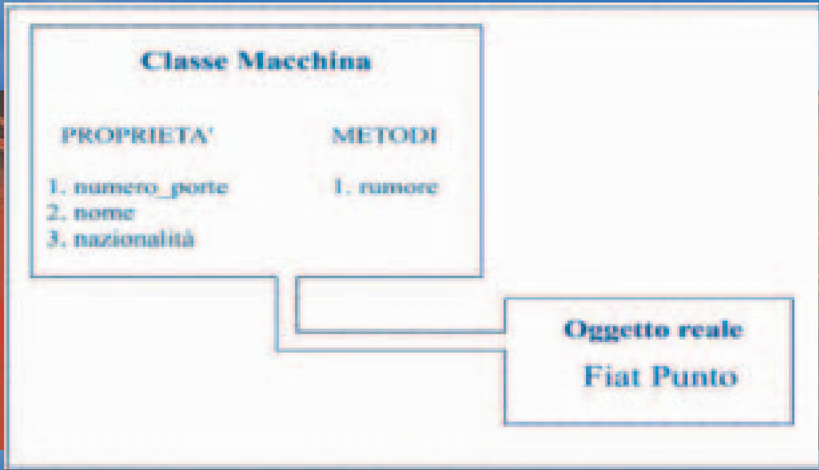
Fino a questo momento abbiamo definito soltanto dati di tipo int. In realtà Java accetta 8 tipi di dati predefiniti. Ci tengo comunque a sottolineare che Java è un linguaggio totalmente orientato agli oggetti, e come tale è possibile definire un numero teoricamente illimitato di nuove categorie di dati. Nel riquadro "Tipi di dati" possiamo vedere quali sono i dati base (o predefiniti) di cui dispone Java:
I più attenti avranno notato che come tipi predefiniti **non sono ammessi né Stringhe nè Array**. In Java infatti questi ultimi sono considerati degli oggetti e quindi vengono definiti dei "tipi personalizzati".

TIPI DI DATI

Tipo	Descrizione
Byte	Intervallo numerico ridotto (8 bit)
Short	Intervallo numerico un pò più ampio rispetto al tipo byte (16 bit)
Int	E' il tipo usato più comunemente per la rappresentazione di interi (32 bit)
Long	Racchiude un vasto insieme numerico (64 bit)
Float	Numero reale di 7 cifre di precisione dopo la virgola
Double	Numero reale di 16 cifre di precisione dopo la virgola
Char	E' il tipo di dato che rappresenta i caratteri Unicode
Boolean	Ammette due valori: TRUE o FALSE

>> Istruzioni di controllo

Per far si che l'utente finale possa interagire col software, il programmatore deve usare dei costrutti che permettono al programma di compiere dei salti all'interno del codice. Questi costrutti prendono il nome di istruzioni di controllo. Vediamo quindi qual' è la loro sintassi:



In questo schema è evidenziata la forte dipendenza tra un oggetto e la sua classe di appartenenza.

```
if ( condizione ) istruzione1;
else istruzione2;
```

Per esempio:

```
if  (numero = = 10) System.out.println ( "
Il numero è 10 ");
else System.out.println (" Il numero non è
10");
```

Beh, in questa porzione di codice possiamo vedere qual' è struttura di fondo che sta dietro al costrutto if-else. Praticamente diciamo al nostro programma che se il valore della variabile numero sarà uguale a 10 stamperà sul monitor la stringa "Il numero è uguale a 10" altrimenti il programma ci indicherà che il numero non è uguale a 10. Se avessimo la necessità di inserire più di una istruzione nel nostro codice **dovremmo necessariamente usare le parentesi graffe:**

```
if (condizione) {
    Istruzione1;
    Istruzione2;
} else {
    Istruzione3;
    Istruzione4;
}
```





Vi presento Duke, la simpatica mascotte che ha sicuramente portato fortuna alla tecnologia Java.

E' anche possibile annidare i nostri costrutti if-else, soprattutto nella realizzazione di applicazioni più articolate

```
if ( condizione) istruzione1;
else if ( condizione2) istruzione2;
else if ( condizione3) istruzione3;
else instruzioneN;
```

>> Istruzioni di iterazione

Queste istruzioni vengono anche chiamate cicli perché fanno si che una porzione di codice venga ripetuta più volte. Comunemente vengono usate due differenti istruzioni di controllo per rappresentare i cicli: while e for. La sintassi dell'istruzione while è while (condizione) { istruzione1; istruzione2; }
In pratica, analizzando questa porzione di codice:

```
int numero =  0;
while (numero < 5) {
 System.out.println("Hacker Journal" );
numero++;
}
```

possiamo notare che per prima cosa definiamo una variabile di tipo int e la poniamo uguale a 0. Poi diciamo alla JVM che finchè (while, appunto…) la variabile numero sarà minore di 5 dovrà stampare a video la stringa "Hacker Journal", e infine, con l'operatore numero ++, la nostra variabile sarà incrementata di 1 ad ogni ciclo. **L' istruzione di iterazione si interromperà quando la condizione sarà falsa**, ovvero quando "numero" sarà maggiore di 5. Lo stesso programma può essere realizzato con l'istruzione **for**. Vediamo la sua sintassi:

```
for ( inizializzazione; condizione;
iterazione) {
   istruzione;
   istruzione;
}
```

Ed ecco come si presenterà la porzione di programma che utilizzerà il costrutto for:

```
int numero;
      for ( numero = 0; numero < 5;
numero++) {
    System.out.println ("Hacker Journal");
}
```

Come vedete all'interno dell'istruzione for abbiamo dapprima inizializzato la variabile, poi abbiamo posto la condizione ed infine l'iterazione. In questo caso **l'output sarà identico a quello dell' esempio precedente ma il codice risulta più leggibile.**



James Gosling parla in pubblico durante un'edizione di JavaOne, il più importante appuntamento per gli sviluppatori Java.

>> Programmazione orientata agli oggetti

Considerando che Java è un linguaggio di programmazione totalmente Orientato agli Oggetti, non potevamo non dedicare spazio a questo argomento. Il costrutto sintattico più importante della programmazione object oriented (Oop) è la **Classe**. Una Classe può essere definita come **un modello per una serie di oggetti che hanno delle caratteristiche comuni**, mentre ogni oggetto rappresenta un'istanza della sua classe di appartenenza. Quando noi definiamo una classe, in pratica, andiamo a creare un nuovo tipo di dato, che può essere tranquillamente manipolato come quelli predefiniti. Come abbiamo avuto già modo di precisare, **in Java i dati di tipo String non sono predefiniti ma sono considerati degli oggetti**. Dunque, per quanto detto, **la classe String rappresenta un modello per ogni oggetto di tipo String**, e di conseguenza, **ogni stringa è una istanza della classe String**. In altre parole, la classe è definita come l'idea di un oggetto, mentre l'istanza è l'oggetto reale. Altri concetti importanti da considerare quando si programma in Java sono quelli di **Proprietà** e **Metodi** degli oggetti. Le proprietà possono essere sia variabili di tipo predefinito che variabili di tipo oggetto, mentre i metodi sono delle azioni, all'interno di un blocco di codice, che l'oggetto esegue quando lo richiamiamo. Per richiamare sia i metodi che le proprietà utilizzeremo la notazione puntata, in questo modo



Da http://java.sun.com si scarica gratuitamente tutto il necessario per programmare in Java.

```
riferimento.nomeProprietà
riferimento.nomeMetodo(argomenti)
```

mentre per definire un metodo utilizziamo la seguente sintassi

```
tipoRestituito nomeMethodo(argomenti) {
 corpo del metodo
}
```

Come sempre, per chiarire meglio le idee, è necessario portare quanto appreso in codice Java…



>> Oop in pratica...

Proviamo adesso a creare un nostro programmino in Java che faccia pieno utilizzo di quanto appreso finora in teoria. Sporchiamoci dunque le mani di codice Java…
Per prima cosa aprite il vostro editor di testo e **create un file con estensione java**, per esempio Macchina.java (il nome del file deve essere uguale a quello della classe). Ecco il codice che va inserito in questo file

```
// Con il costrutto class definiamo un
nuovo tipo di dato
class Macchina {
   // Proprietà che rappresenta il numero
di porte dell'auto
   int numero_porte;
   // Proprietà con il nome dell'auto
   String nome;
   // Proprietà con la nazione dell'auto
   String nazionalità;
   // Metodo che esprime un'azione che
l'oggetto auto può compiere
   void rumore() {
      System.out.println (" Brum brum
brum... ");
   }
}
```

Le stringhe che iniziano con // costituiscono i commenti al codice, che il compilatore non considera, ma che garantiscono una maggiore leggibilità del codice stesso. Come vedete abbiamo così definito un nuovo tipo di dato, che funge da modello per ogni oggetto Macchina. **Salviamo il nostro file e creiamone un altro col nome MacchinaTest.java**

```
class MacchinaTest {
   //Definiamo il metodo main() che consente
l'esecuzione del programma
   public static void main( String args[] )
{
      // creiamo un nuovo oggetto di tipo
Macchina
      Macchina macchinaMia = new Macchina();
      //usiamo la notazione puntata per
attribuire le proprietà all'oggetto
      macchinaMia.nome = "Fiat Punto";
      macchinaMia.numero_porte = 5;
      macchinaMia.nazionalità = "italiana";
      System.out.println (" La mia macchina
e' una " + macchinaMia.nome +".");
      System.out.println (" E' una macchina
a " + macchinaMia.numero_porte + "
porte.");
      System.out.println (" Inoltre e' una
macchina " + macchinaMia.nazionalità +".");
                          System.out.println
(" Quando la accendo fa: ");

      // Richiamo il metodo rumore(), sempre
con la notazione puntata
      macchinaMia.rumore();
   }
}
```

In questo file invece abbiamo definito un 'istanza della classe Macchina. Potete vedere come sono stati usati i metodi e le proprietà attraverso la notazione puntata. Adesso ponete i due file all'interno di una cartella che andremo a creare e compilate il file MacchinaTest.java con il comando

```
javac MacchinaTest.java
```

Il compilatore rileva automaticamente le dipendenze con la classe Macchina e darà come output il bytecode con estensione .class. Per eseguire il nostro programma basterà digitare dal prompt del dos il comando

```
java MacchinaTest
```

senza specificare l'estensione del bytecode. L'output prodotto sarà il seguente

```
  La mia macchina è una Fiat Punto.
  È una macchina a 5 porte.
  Inoltre è una macchina italiana.
  Quando la accendo fa:
  Brum brum brum…
```

Antonino Benfante



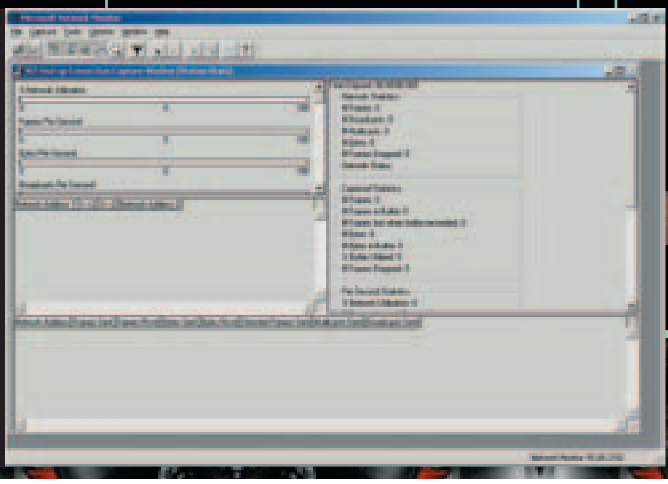
COME RINTRACCIARE L'AUTORE DI UN ATTACCO AI NOSTRI DANNI

SIAMO ATTACCATI !

Vediamo come rendere la vita un inferno a chi cerca di invadere il nostro orticello informatico.

Quest'articolo descrive le tre fasi in cui si può dividere un intervento che segue ad un attacco informatico. Questa è la prima domanda cui è necessario rispondere quando si subisce un attacco è: **"che cosa sta succedendo?"**. Infatti, non sempre dai sintomi di malfunzionamento è possibile individuare immediatamente la modalità ed il target dell'attacco, soprattutto se ci troviamo in una rete di medie o grandi dimensioni. **La prima cosa da fare è effettuare un trap and trace per individuare quale punto del nostro sistema è sotto attacco**.

Il trap and trace consiste nell'**analisi del traffico di rete passante per un singolo host o per un intero segmento di rete** qualora quest'ultimo sia dotato di hub broadcast, cioè hub che trasmettono gli stessi pacchetti a tutti gli host collegati; saranno poi i destinatari ad effettuare una selezione sui pacchetti. I tool che si possono utilizzare sono **tcpdump** per linux o **WinDump** (il corrispondente di tcpdump per Windows), che sono a linea di comando. Chi preferisce usare un programma con interfaccia grafica, può usare **netmon** sempre per Windows. L'utilizzo di questi tool per l'intrusion detection è sicuramente **poco pratico ma necessario quando gli IDS automatici non sono efficaci**, o perché l'attacco non viene riconosciuto, o perché l'IDS viene completamente bypassato. Sono molto in voga in questo periodo alcune tecniche di programmazione di virus e trojan il cui scopo è la disattivazione o inibizione dei servizi antivirus e IDS.



>> Usare e capire tcpdump

Per il nostro esempio utilizzeremo **tcpdump**. Una volta installato su linux con la solita procedura (./configure, make, make install), tcpdump può essere avviato semplicemente richiamando l'eseguibile da una shell di root. Se si utilizza senza opzioni, l'applicazione visualizza sulla finestra di shell tutto il traffico che attraversa la scheda di rete. Questo può essere utile nella primissima fase. **Per fare in modo che l'output sia un file di testo più facilmente consultabile** basta avviare tcpdump in questo modo:

```
./tcpdump > fileditesto
```

L'output del tcpdump non sono altro che i primi n byte (**di default 68**) di ogni pacchetto dati. All'incirca ciò corrisponde a qualcosa in più delle intestazioni dei pacchetti che varia dai 28 byte per quelli UDP ai 40 byte per i TCP. I dati catturati si presentano come potete vedere in figura.

Il primo campo, cioè il timestamp, indica l'attimo esatto in cui è stato costruito il pacchetto; subito dopo troviamo gli **indirizzi sorgente e destinazione** con le relative porte utilizzate (notate il simbolo ">" che indica la direzione della connessione). Dopo abbiamo **i flag TCP** che ci danno informazioni sul tipo di pacchetto (tutti i flag con i relativi significati potete trovarli in un sito indicato tra i link). Potete inoltre vedere il campo che ci dice **di quanti pacchetti è costituita la comunicazione** e l'**ID del pacchetto** presente. Infine, **l'indice di frammentazione** ci dice se il pacchetto è integro. Questo può essere utile per individuare certi tipi di attacchi detti appunto a frammentazione di pacchetto utilizzati in genere per superare i firewall. Detto questo, al fine di effettuare un'analisi efficace senza perdersi nell'infinità dei dati è opportuno porsi le seguenti domande:

I campi delle intestazioni IP sono sospetti? Ossia l'indirizzo Ip di origine è sospetto (vedremo poi come verificarne la provenienza)? Vi sono frammentazioni anomale dei pacchetti? La dimensione del pacchetto è eccessiva?

Sono sospetti i campi delle intestazioni TCP? La porta di destinazio-

ne non corrisponde ad un servizio attivo sul vostro sistema?
Il traffico è conforme alle norme di quel particolare protocollo? Se per esempio vediamo una serie di pacchetti con flag SYN consecutivi relativi alla stessa comunicazione è probabile che ci si trovi di fronte ad un SYN flooding poiché non viene rispettato l'handshake normale.

>> I log dei servizi attaccati

Se in questo modo riuscite a individuare il servizio attaccato, allora potete **passare alla fase successiva e cioè all'analisi dei log del singolo servizio,** non senza però prima esservi annotati l'ip o gli ip sospetti. Se per esempio stiamo utilizzando un server windows 2000, e sappiamo che l'attacco ha colpito IIS, possiamo trovare i suoi log nella cartella **winnt/system32/logfiles**. Qui, attraverso una semplice ricerca sul testo degli ip precedentemente trovati, **possiamo ricostruire tutte le operazioni svolte dagli attaccanti**, scoprire quale vulnerabilità è stata utilizzata e possiamo tappare facilmente il buco applicando la patch appropriata. Supponiamo, infatti, di avere dei log come questi:

```
2003-04-17 15:25:58
192.168.0.10 - 192.168.0.2
80 GET
/scripts/../../winnt/system
32/cmd.exe /c+dir+c:\ 200 -
2003-04-17 15:25:58
192.168.0.10 - 192.168.0.2
80 GET
/_vti_bin/../../../../../..
/winnt/system32/cmd.exe
/c+dir+c:\ 200 -
```

Questi sono **due tentativi riusciti di accedere alla visualizzazione su browser della directory c:\ del server** attraverso la vulnerabilità Unicode di IIS (notate la restituzione del codice 200 'OK' da parte del server invece del 404 'not found').

>> Risalire all'origine

Una volta individuato l'ip di provenienza di un attacco ci si trova di fronte a due possibilità:
Se l'attacco è di tipo DOS (come i SYN flooding, gli attacchi a frammentazione di pacchetto) e quindi non sempre richiede il completamento dell'handshake di connessione, **è molto probabile che l'ip sia fasullo.**
Se invece avete subito un attacco di altro tipo, come per esempio gli attacchi ai singoli servizi (WEB, FTP, Posta, etc) **allora avete un ip da cui cioè è partito o è passato l'attacco che è quantomeno esistente**.
Nel primo caso purtroppo risalire all'origine è molto difficile se non impossibile anche se l'entità del danno provocato in realtà è molto ridotta.
Nel secondo caso **si può cominciare effettuando un traceroute per individuare l'area geografica cui appartiene l'ip**. Per il traceroute potete utilizzare il comando **traceroute** (per Linux) o **tracert** (per Windows) seguito dall'ip che avete trovato sul file di log. In genere gli host attraversati hanno nel loro DNS un indicativo del luogo in cui si trovano come potete vedere nel riquadro "Tracciare l'attaccante".

TRACCIARE L'ATTACCANTE

Risultato del tracciamento di un indirizzo ottenuto con tracert su Windows, partendo da un nodo di una sottorete locale (indirizzo 192.168.0.1), e arrivando a Roma passando per Napoli, Roma, Milano e poi arrivando a destinazione nuovamente a Roma. Le città si possono dedurre dai nomi dei nodi dei grossi provider, che solitamente contengono la sigla della provincia.

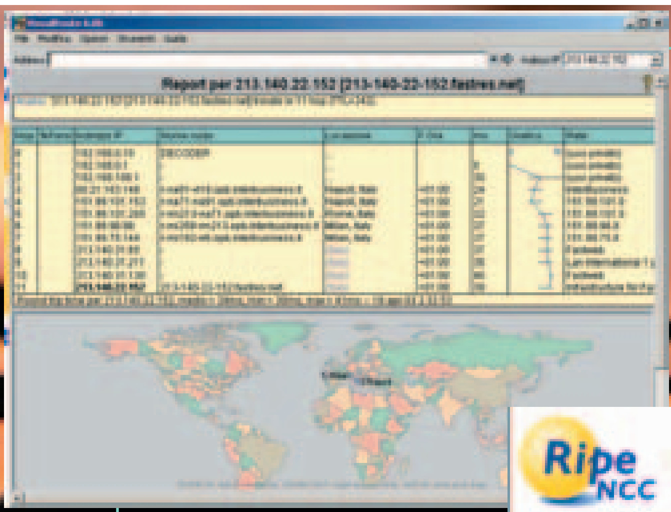
```
C:\>tracert www.wind.it

Rilevazione instradamento verso www.wind.it [212.141.84.128]
su un massimo di 30 punti di passaggio:

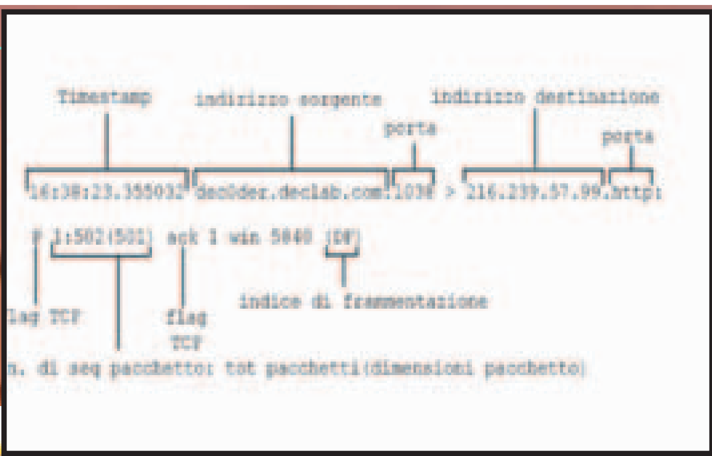
  1 <10 ms <10 ms <10 ms  192.168.0.1
  2  30 ms  30 ms  30 ms  192.168.100.1
  3  30 ms  30 ms  20 ms  r-na90-vl19.opb.interbusiness.it [80.21.163.147] <- NA
  4  30 ms  30 ms  30 ms  r-na70-na90.opb.interbusiness.it [151.99.101.137]
  5  30 ms  30 ms  40 ms  r-rm215-rm70.opb.interbusiness.it [151.99.101.209]<-RM
  6  40 ms  40 ms 40 ms  r-mi256-rm215.opb.interbusiness.it [151.99.98.10 2]<-MI
  7  40 ms  40 ms  50 ms  151.99.75.163
  8  40 ms  50 ms  40 ms  80.17.211.198
  9  40 ms  50 ms  40 ms  wind2-mix.mix-it.net [217.29.67.43]
 10  50 ms  60 ms  60 ms  c-rm6-mix2-pos.wind.it [212.245.250.29]<-ROMA
 11  50 ms  60 ms  50 ms  c-rm42-rm1-fe6a.wind.it [212.245.158.159]
 12  50 ms  60 ms  50 ms  c-elan-rmgio1-rm42.wind.it [212.245.153.42]
 13  50 ms  60 ms  60 ms  212.141.84.128

Rilevazione completata.
```

COME RINTRACCIARE L'AUTORE DI UN ATTACCO AI NOSTRI DANNI



Dai risultati potete avere informazioni importanti riguardanti il sistema da cui siete stati attaccati, come il responsabile tecnico e amministrativo, e soprattutto chi si occupa degli abusi della rete. Nel caso in esame scoprirete che il range cui appartiene l'ip è di FastWeb:





Come potete notare qui sono facilmente individuabili i nodi geografici. Per rendere comunque il tracing più comodo è **possibile utilizzare tool visuali che indicano su una mappa la collocazione dei vari host,** come per esempio VisualRoute (www.visualware.com). Una volta individuata l'area geografica di provenienza dell'ip, allora **potete effettuare un'interrogazione whois ai RIR** (Regional Internet Registry) in base all'area geografica cui appartiene il vostro target: il RIPE (Réseaux IP Européens) per l'Europa, parte dell'Africa e il Medio Oriente; l'ARIN (American Registry of Internet Numbers) per l'America settentrionale e meridionale, i Caraibi e l'Africa sub-Sahariana; infine l'APNIC (Asia Pacific Network Information Center) per il resto dell'Asia e il Pacifico. **Se utilizzate sistemi Microsoft potete consultare direttamente i siti di questi tre enti** oppure utilizzare delle utility come **Sam Spade** (tutti gli indirizzi sono nel riquadro in queste pagine). **Per i linuxari è sufficiente l'utility whois** di cui è dotato il sistema operativo. Se ad esempio vogliamo sapere a chi appartiene l'IP 213.140.22.152, sapendo però che l'area geografica in cui si dovrebbe trovare l'host è l'Europa, basta lanciare dalla shell questa linea di comando:

```
whois
213.140.22.152@whois.ripe.n
et
```

```
inetnum:
213.140.22.144 -
213.140.22.159
netname:       FASTWEB-POP-
0115-RESIDENTIAL
descr:
Infrastructure for
Fastweb's main location
descr:            NAT IP
addresses for residential
customer, public subnet
country:       IT
```

e che esiste un reparto per il controllo degli abusi:

```
remarks:       In case of
improper use originating
from our network,
remarks:       please mail
customer or
abuse@fastweb.it
```

A questo punto non vi resta che raccogliere il materiale della vostra indagine (log e amenità varie) e **inviarlo all'indirizzo** abuse@fastweb.it. **Saranno loro a verificare** se l'attacco è nato dalla loro rete o la ha soltanto attraversata. Aggiungo che in generale, quasi per convenzione, le mail di riferimento in casi di questo tipo sono sempre abuse@dominioprovider. In genere, qualora l'attacco non sia stato intrusivo, ad azioni di questo tipo segue **un semplice avvertimento da parte del provider** all'utente. A questo però può seguire la **sospensione del servizio nel caso in cui il colpevole sia recidivo o la denuncia alla magistratura qualora l'attacco abbia portato a un danno.**

Roberto 'dec0der' Enea
enea@hackerjournal.it

LINK UTILI

Tcpdump
http://www.tcpdump.org
Un articolo in cui sono indicati i TCP flag
http://linux.oreillynet.com/pub/a/linux/2001/06/29/tools_two.html
WinDump
http://netgroup-serv.polito.it/windump
ARIN
http://www.arin.net
RIPE
http://www.ripe.net
APNIC
http://www.apnic.net
Sam Spade
http://www.samspade.org
VisualRoute
http://www.visualware.com



NEWBIE

COME VEDERE I FILM IN DIVX CON DREAMCAST



I FILM SULLA CONSOLE

Stufi di vedere video su un monitor piccolo e sulla sedia della Scrivania? Non sarebbe meglio la TV e un bel divano? Ecco come fare usando un masterizzatore e il Sega Dreamcast.



Non c'è bisogno di presentare il codec DivX, che si è imposto come il più efficace e universale metodo per la compressione di filmati. Con il codec DivX, è possibile comprimere un film di più di un'ora nello spazio di un cd.

Certo, se io volessi guardare quel film su uno schermo televisivo **dovrei avere a disposizione una scheda video con TV-OUT** ed un cavo abbastanza lungo che mi permetta di raggiungere la TV in salotto.

Ma se non avessi tutto ciò? Se tutto quello di cui disponessi fosse un computer con un masterizzatore?

Ci sarebbe ben poco da fare se non comprare una nuova scheda video, oppure un lettore di DVD compatibile con il formato DivX (ce ne sono un paio, e costano mezzo stipendio). **In realtà l'alternativa c'è: spendere qualche decina di Euro per comprare una Dreamcast usata** (e possibilmente già modificata per la compatibilità coi giochi NTSC) e scaricare da Homebrew il DCDivX 4 Dummies (http://homebrew.dcemulation.com/zacmcd/DcDivX4dummies/DcDivX4Dummies.zip)

> **?** Codec: Abbreviazione di compressor/decompressor; una qualsiasi tecnologia in grado di comprimere e decomprimere dati.

>> La soluzione

In questo piccolo file ZIP sono contenuti alcuni tool che permettono di creare un immagine per NERO Burning ROM di un disco avviabile dalla DreamCast e contenente il **DCDivX player** e i filmati che vi interessa vedere. Per farlo basta decomprimere il file Zip in una directory qualsiasi (per esempio C:\Dcdivx4dummies) e inserire i filmati nella sottodirectory Dcdivx (quella che contiene il file 1st_read.bin). Fatto questo **avviate il file batch makenero.bat** e alla fine della procedura avrete un file Dcdivx.nrg, ovvero **un'immagine masterizzabile con NERO.** Infilate un CD-R nel masterizzatore e fate doppio clic sull'immagine; NERO effettuerà la copia e a voi non resterà che provare il risultato infilando il CD nella console e accendendola.

>> Alcune raccomandazioni

Il sistema funziona bene, ma ha alcuni limiti. Vediamoli:

1 **Non si devono superare i limiti imposti dallo standard ISO-9660** ovvero 650 megabyte, altrimenti i risultati potrebbero essere imprevedibili.

2 I filmati devono essere in **low resolution (320x240) e il bit rate non deve essere troppo elevato**. Questo perché la DreamCast ha un processore a 200 MHz e solo 16 Megabyte di RAM (e per quello per cui è stata progettata sono più che sufficienti).

3 **Non aspettatevi grandi risultati**, questa è una soluzione di ripiego, ideale se si vuol vedere un DivX da un amico che non ha il computer e non si ha un portatile con uscita TV-OUT.

Skyglobe

